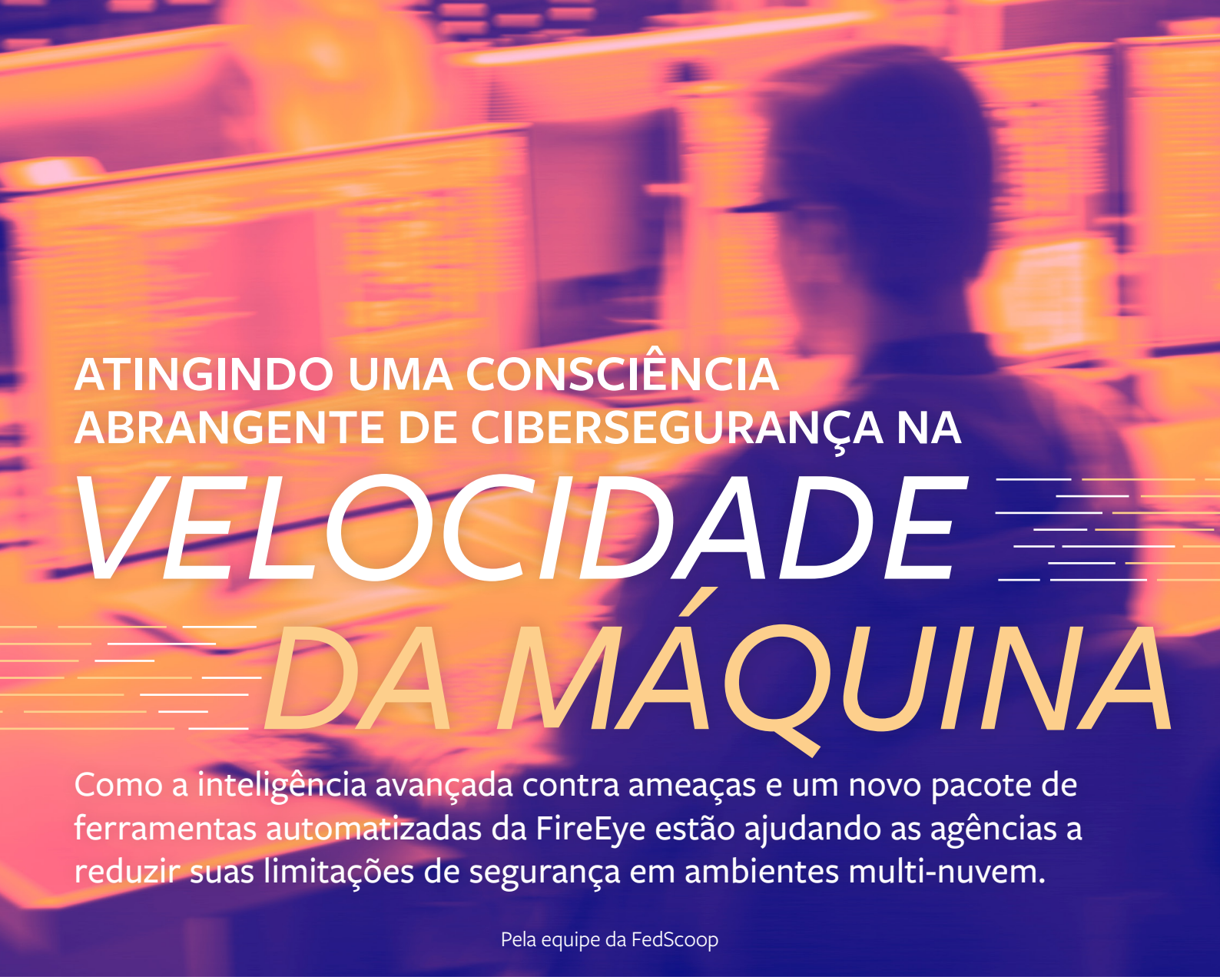

# ATINGINDO UMA CONSCIÊNCIA ABRANGENTE DE CIBERSEGURANÇA NA *VELOCIDADE DA MÁQUINA*

Como a inteligência avançada contra ameaças e um novo pacote de ferramentas automatizadas da FireEye estão ajudando as agências a reduzir suas limitações de segurança em ambientes multi-nuvem.

Pela equipe da FedScoop

**RON BUSHAR, CTO PARA GOVERNO NA FIREEYE,** viu sua cota de casos de ransomware e violações de segurança nos últimos 12 meses. A cena é familiar. Ele e os analistas da FireEye se reuniam - lado a lado - com membros da equipe de segurança de uma agência governamental para avaliar com o que estavam lidando. O FBI normalmente estaria lá - às vezes, o Serviço Secreto também - junto com especialistas de vários fornecedores de tecnologia de segurança.

Em anos anteriores, a FireEye fez parceria com a Mandiant para investigar violações de segurança cibernética: A FireEye era a empresa na qual as grandes corporações confiavam para identificar uma violação de segurança; a Mandiant, adquirida pela FireEye em 2013, era a empresa que poderia dizer quem eram os hackers e como responder. Desde então, os especialistas de resposta a incidentes e de inteligência responderam a dezenas de milhares de violações em todo o mundo.

A FireEye ganhou sua reputação por ter capacidade de detectar explorações globais de atacantes - e por fornecer ferramentas automatizadas para detectá-los e lidar com eles rapidamente. Essa reputação continuou a crescer com uma série de aquisições, incluindo a mais recente, a Verodin (conhecida atualmente como Mandiant Security Validation), provedor de serviços de instrumentação de segurança, e a Cloudvisory, que fornece visibilidade de segurança em ambientes multi-nuvem.

"A FireEye pode entrar e implantar agora o que sabemos sobre cada variante de ransomware que estamos vendo ao redor do mundo e começar a procurá-la em minutos, independentemente da tecnologia que a agência está usando", diz Bushar. "Imediatamente, podemos dizer: 'É esse grupo. Essas são as técnicas que eles usam. É assim que conseguem acesso. É aqui que devemos procurar para encontrar onde eles implementaram seu ransomware. E essa é a melhor maneira de agir para isolar a ameaça e conseguir que os sistemas voltem a funcionar'."

*Suas informações não podem mais ficar meses ou semanas desatualizadas.*
*E você também precisa combiná-las com agilidade no lado da tecnologia e conseguir trabalhar em escala.*

**RON BUSHAR**,
CTO para Governo na FireEye

Porém, Bushar reconhece que a evolução dos ataques cibernéticos é apenas parte do desafio que os agentes do governo enfrentam. Também há uma pressão implacável para modernizar seus sistemas de TI antigos em meio a restrições de recursos de longa data.

"As agências têm o mesmo problema de capacidade que todos têm para manter um conjunto talentoso de habilidades. E todos estão sobrecarregados, certo?", disse Bushar, que atuou como ex-diretor assistente do Departamento de Justiça para operações de segurança antes de assumir cargos importantes na Mandiant e FireEye.

A boa notícia, diz ele, é que uma combinação de fatores agora possibilita que as agências obtenham uma visibilidade muito maior em suas redes - tanto local quanto na nuvem - e também reduz drasticamente o tempo que leva para detectar e bloquear ameaças potenciais.

## ALCANÇANDO VISIBILIDADE ABRANGENTE

Independentemente de onde as agências estão em termos de esforços de modernização de TI, a migração contínua para serviços na nuvem as forçou a transformarem o modo de pensar sobre segurança.

Embora muitas agências federais ainda devam manter controles de perímetro definidos estaticamente, esses controles estão em grande parte voltados para a prevenção em vez da detecção. Migrar dados e aplicativos para a nuvem requer soluções fundamentalmente diferentes para gerenciar a segurança em um ambiente distribuído, mais dinâmico e mais diverso.

Também existe o que o major general Earl Matthews (aposentado da Força Aérea dos Estados Unidos), Vice-Presidente de Estratégia da Mandiant Security Validation, chama de "movimentação do ambiente".

"Sistemas e aplicativos de TI mudam diariamente. Novos aplicativos são implantados; ferramentas são atualizadas; há mudanças de equipamento", diz Matthews. "Se todo o seu ambiente de TI está em mudança diariamente, a pergunta que precisa ser respondida é: Seus sistemas de controle de segurança estão acompanhando, e como você pode ter certeza?"

A resposta começa em suprir as deficiências de visibilidade, insiste Martin Holste, CTO de Nuvem da FireEye.

"Tudo depende da visibilidade em um ambiente distribuído", ele destaca. "Ela é o alicerce fundamental de qualquer estratégia de segurança na nuvem, quer a estratégia gire em torno da garantia de conformidade, busca de ameaças, governança de políticas ou remediação de riscos".

Sobretudo, "as agências também precisam ampliar a habilidade de detectar e responder a ameaças na velocidade da máquina, principalmente à medida que migram para a nuvem", ele diz.

Alcançar essa visibilidade continua a ser uma grande dificuldade e uma necessidade urgente para a maioria das grandes corporações: 43% dos profissionais de vários setores, incluindo o setor governamental, definiram a "visibilidade na segurança da infraestrutura" como o principal problema enfrentado atualmente, de acordo com o Relatório de Segurança na Nuvem de 2020 da Cyber Security Insiders.

A visibilidade abrangente na segurança da infraestrutura requer várias formas de visibilidade simultaneamente, de acordo com Holste. Isso inclui ter:

- **Um inventário completo de todos os ativos relevantes o tempo todo.** Sem um inventário atualizado e com o registro histórico de todos os ativos em escopo, as auditorias de conformidade e a análise de segurança produzirão resultados incompletos e/ou enganosos.

- **Detalhes contextuais sobre a situação atual de cada ativo.** Sem a visibilidade no contexto de todo e qualquer ativo, e a capacidade de buscar esses detalhes quando necessário, não há significado e validade em conceitos como garantia de conformidade e detecção de anomalias.
- **O registro histórico completo dos eventos de segurança de cada ativo**. Sem visibilidade do comportamento real das cargas de trabalho (workloads) e dos usuários, não existe uma maneira de confirmar se as políticas de governança estão funcionando ou se os invasores já não tomaram uma parte da sua infraestrutura.

De acordo com Holste, a solução Cloudvisory proporciona às agências a capacidade de monitorar mais profundamente vários ambientes na nuvem, assim como cargas de trabalho (workloads) contidas quanto a possíveis vulnerabilidades e ameaças. Ela também funciona com uma ampla variedade de tecnologias de segurança e com todos os prestadores de serviço de nuvem líderes. E ela oferece aos usuários controles automatizados e regras de políticas que podem ser entregues na velocidade da máquina para que as agências consigam ajustar continuamente suas políticas de segurança à medida que as operações continuem a evoluir no futuro.

Sempre que um desenvolvedor cria um novo serviço na nuvem, por exemplo, ele precisa ser capaz de centralizar facilmente a telemetria, para proporcionar aos analistas a capacidade de ir a um único local para analisar a situação de segurança de todos os serviços na nuvem.

## ADAPTANDO A SEGURANÇA A UMA FORÇA DE TRABALHO REMOTA

Justamente quando muitas equipes de segurança corporativa estavam se acostumando a gerenciar a segurança em ambientes de TI distribuídos, de repente tiveram que enfrentar uma nova força de trabalho distribuída.

Isso significou não apenas adaptar seus controles de monitoramento e detecção de segurança para acomodar um aumento no número de funcionários trabalhando remotamente, mas também ter que executar essas funções de segurança remotamente. Ter um conjunto robusto de ferramentas analíticas e de detecção - que pode monitorar e aplicar políticas de segurança, detectar novos tipos de vulnerabilidades e distinguir entre mudanças de comportamento e comportamento incomum - tornou-se mais importante do que nunca.

Adições recentes na plataforma de análise FireEye Helix tornaram isso possível, por exemplo, para identificar comportamento de logon de VPN anormal mais rapidamente, de acordo com Gregory Smith, Gerente Sênior de Marketing de Produtos na FireEye. Empresas que adotam pacotes de produtividade na nuvem, como o Office 365, conseguem medir e detectar automaticamente comportamento atípico.

Porém, responder a ameaças cibernéticas continua a ser um negócio complicado e cuja complexidade é crescente, diz Bushar.

"É necessária uma combinação de experiência e conhecimento do ambiente de ameaças em tempo real, assim como da infraestrutura de TI e da maneira como ela evoluiu com o passar do tempo. Suas informações não podem mais ficar meses ou semanas desatualizadas. E você também precisa combiná-las com agilidade no lado da tecnologia e conseguir trabalhar em escala", ele diz.

Ele dá crédito à divisão Mandiant Threat Intelligence da FireEye, que consegue identificar quais agentes de ameaça estão mais propensos a se interessarem por determinada empresa, para ajudar os executivos de segurança da informação a melhorarem suas defesas. Além disso, a Mandiant Security Validation proporciona aos CISOs ferramentas de instrumentação para ajudar a gerenciar e comunicar riscos de segurança à gestão sênior e oferecer uma justificativa mais clara para investimentos de TI e segurança.

*"Tudo depende da visibilidade em um ambiente distribuído. As agências também precisam ampliar a habilidade de detectar e responder a ameaças na velocidade da máquina, principalmente à medida que migram para a nuvem."*

**MARTIN HOLSTE**,
CTO de Nuvem na FireEye,

## ECOSSISTEMA FIREEYE


*O Ecossistema FireEye combina tecnologia e experiência para alcançar a melhor postura de segurança por meio de um pacote completo de recursos de detecção, proteção e resposta. Isso inclui soluções de segurança de rede, endpoint, e-mail e nuvem em uma plataforma de operações de segurança, a Helix. O ecossistema também inclui uma plataforma de instrumentação, a Mandiant Security Validation, que mede, testa e melhora continuamente a eficácia da segurança cibernética. Por fim, os serviços Mandiant Consulting, Managed Defense e Threat Intelligence incrementam as empresas com os recursos e tecnologia necessários para responder e proteger as organizações contra as ameaças mais avançadas.*

*Fonte: FireEye*

No entanto, o objetivo real, ele diz, é gerar visibilidade e percepções de maneiras sobre as quais os clientes da FireEye possam agir.

"Se você conversar com qualquer um que trabalhe na área de inteligência de ameaças", observa Bushar, "a reclamação número um não é que as pessoas não estão fornecendo inteligência suficiente. É o fato de estarem fornecendo em excesso.
No entanto, a segunda coisa que eles dizem é: 'Eu sequer consigo utilizá-la de uma forma que seja útil para mim', ou eles não sabem o que fazer exatamente com as informações. O que estamos tentando fazer agora com nossa função de inteligência é ir além do relatório legível para pessoas, o que ainda é útil, e aplicar essa inteligência na velocidade da máquina... mas fazendo isso de uma forma que possibilite de fato a análise proativa e preditiva".

"Em um nível elevado, realmente estamos tentando possibilitar, do modo mais rápido e homogêneo possível, tudo o que sabemos sobre os adversários, suas ferramentas, técnicas, motivações e objetivo, e levar isso aos nossos clientes de uma forma que eles queiram consumir, na velocidade da máquina", diz Bushar.

*Saiba mais sobre o pacote completo de detecção, proteção e de recursos de resposta da FireEye com soluções de segurança de rede, endpoint, e-mail e nuvem, assim como uma plataforma de operações de segurança, Helix, e nossos serviços Mandiant Security Validation, Mandiant Consulting, Managed Defense e Threat Intelligence.*

fedscoop FIREEYE