IBM Security MaaS360 with Watson

Proteja seus endpoints com gerenciamento de ameaças de classificação corporativa

Destaques

Aproveite a IA e a análise de segurança desenvolvidas com Watson

Proteja os dados corporativos com políticas de segurança robustas

Tenha detecção e correção avançadas de ameaças

Integre o suporte SIEM, SOAR e IAM

No mundo atual, em que é possível trabalhar de qualquer lugar, as organizações buscam gerenciar de forma centralizada os endpoints e a segurança, criar experiências sem atrito para seus usuários finais, reduzir ameaças cibernéticas e manter os custos de propriedade baixos. As empresas enfrentam desafios com várias ferramentas e dashboards de segurança de endpoint, que podem limitar a capacidade dos analistas de segurança e dos administradores de TI de serem eficazes na mitigação e no tratamento de ameaças. Por exemplo, o relatório anual sobre o Custo da Violação de Dados da IBM, que apresenta pesquisas do Ponemon Institute, afirma que o custo total médio global de uma violação de dados entre as organizações pesquisadas aumentou 2,6%, de US$ 4,24 milhões em 2021 para US$ 4,35 milhões em 2022. Este foi o maior número na história deste relatório, sendo que 83% das organizações estudadas sofreram mais de uma violação de dados.[1]

O IBM Security MaaS360 with Watson é uma solução unificada de gerenciamento de endpoint (UEM) que teve seus recursos integrados de gerenciamento de ameaças evoluídos de um pequeno conjunto de detecções até a inclusão de uma nova política centralizada e de um conjunto mais amplo de detecções e respostas para ameaças, como e-mail e phishing por SMS, bem como ameaças internas. Ele foi projetado para ajudar as organizações a mesclar eficiência e eficácia ao gerenciar endpoints, incluindo dispositivos móveis, notebooks, desktops, dispositivos vestíveis e dispositivos robustos, além de ajudar a protegê-los com recursos aprimorados de gerenciamento de ameaças. Esses recursos de gerenciamento de ameaças são integrados ao produto para ajudar as empresas a atingir os níveis de custo total de propriedade desejados.

Detecção e correção de ameaças evoluídas
De acordo com a Pesquisa de Gerenciamento e Segurança do Espaço de Trabalho Corporativo da IDC para 2021, o phishing de e-mail móvel e o phishing de SMS foram identificados pelos administradores de segurança e TI dos EUA como as duas principais ameaças de segurança móvel mais frequentes[2].

O IBM Security MaaS360 with Watson expandiu seus recursos de gerenciamento de ameaças com um conjunto de detecções e respostas para incluir casos de uso de ameaças internas móveis, ameaças internas de maior valor e detecções de zero trust. O MaaS360 with Watson consolida a política e a definição de resposta em uma política centralizada, aprimora o dashboard de risco em um dashboard de análise de segurança de função completa e fornece oportunidades de integração baseadas em API. Tudo isso combinado com acesso condicional baseado em risco para automatizar as respostas às ameaças.

Além da proteção contra malware, dispositivos com jailbreak feito e roteados e Wi-Fi inseguro, o MaaS360 with Watson também oferece detecção de phishing por SMS e e-mail, excesso de permissões de aplicações para dispositivos Android, gerenciamento de privilégios para usuários de Windows e MacOS e ameaças baseadas em configuração de dispositivo para dispositivos Android. O MaaS360 with Watson pode ser integrado à maioria dos fornecedores terceirizados existentes caso sua organização já possua um software sofisticado de gerenciamento de ameaças.

Defina políticas de segurança robustas ou escolha políticas predefinidas para defender os dados corporativos
O IBM Security MaaS360 with Watson possui uma política de segurança de endpoint central atualizada que pode controlar detecções e respostas para vários tipos de ameaças. O MaaS360 with Watson inclui políticas para casos de uso, como detecção de dispositivos com jailbreak e roteados baseados em assinatura, detecção de phishing de troca IBM® X-Force (e-mail e SMS), detecção de permissão excessiva de aplicações, detecção de malware e Wi-Fi inseguro e detecção de privilégios de processos e usuários do Windows e MacOS.

Além dos tipos comuns de ameaças cibernéticas, um administrador de TI tem outras prioridades com que se preocupar, como gerenciar a devolução de dispositivos corporativos ou auxiliar funcionários que perdem seus dispositivos. Para esses casos, um administrador pode estabelecer um local sob demanda, que permite recuperar dispositivos perdidos ou roubados e detectar anomalias geográficas de dispositivos de usuários que possam ter sido comprometidos. Os administradores também se beneficiam do suporte à criptografia e podem habilitar ações automatizadas, de alertas básicos à limpeza seletiva de recursos corporativos, até que os problemas sejam corrigidos.

Aproveite a IA e a análise de segurança desenvolvidas com Watson
A análise e os dashboards de segurança são uma parte importante das soluções modernas de UEM. O IBM Security MaaS360 with Watson fornece análises e insights impulsionados por IA, usando dados estruturados e não estruturados, bem como análises comportamentais aplicadas para fornecer insights e recomendações de ações automatizadas.

O mecanismo de recomendação de políticas usa análises de dados do cliente para recomendar alterações individuais nas políticas que podem ser mais adequadas à organização. Os dashboards de segurança foram aprimorados para se adequar aos recursos de gerenciamento de ameaças evoluídos. As detecções são exibidas no Dashboard de segurança na seção Incidentes de segurança. Esses incidentes de segurança também estão disponíveis por meio da API de segurança e são usados para calcular uma pontuação de risco com base nas regras de risco. Relatórios granulares, incluindo atividade do dispositivo, aplicação e uso de dados para o software instalado, também são fornecidos.

O MaaS360 with Watson também aplica automatizações para que os administradores de TI possam agendar e-mails para enviar relatórios sobre parâmetros específicos de forma diária, semanal ou mensal para manter-se atualizado sobre importantes estatísticas organizacionais.

Integre o suporte SIEM, SOAR e IAM
As tecnologias de gerenciamento de eventos de informações de segurança (SIEM) e operações de segurança, automação e resposta (SOAR) tornaram-se parte de posturas de segurança robustas de organizações em todo o mundo. O MaaS360 with Watson ampliou suas integrações com essas tecnologias e criou uma nova API que fornece eventos de incidentes e dados gerados pelo MaaS360 para sistemas de terceiros. O MaaS360 integra-se perfeitamente com o IBM QRadar para oferecer uma experiência de segurança de ponta a ponta em que todos os incidentes detectados estão disponíveis para visualização por meio de uma origem de log pré-empacotada que é facilmente configurada.

O gerenciamento de identidade e acesso (IAM) é extremamente útil para empresas que desejam proteger suas informações corporativas, concedendo acesso granular aos recursos certos, mantendo a conformidade com os padrões da empresa e do setor.

O MaaS360 conta com uma página inicial unificada para SSO corporativo e pode fornecer qualquer aplicação corporativa para uso com a barra de ativação de identidade ou catálogo de aplicações unificado. As políticas de acesso condicional baseadas em risco podem ser configuradas para ajudar a impedir que usuários e dispositivos arriscados interajam com dados confidenciais ou outros recursos corporativos. O Maas360 também se integra ao IBM Security Verify para oferecer recursos de identidade da força de trabalho e identidade do cliente ou com o provedor de identidade baseado em padrões existente a fim de fornecer suporte a recursos de acesso condicional. O Maas360 with Watson inclui autenticação de diversos fatores, que pode ser implementada em aplicações SaaS específicas e oferece suporte a vários fatores secundários.

Conclusão
O MaaS360 with Watson oferece automação, gerenciamento de endpoint moderno e recursos integrados de gerenciamento de ameaças que ajudam a proteger contra ameaças cibernéticas, como phishing, ataques man-in-the-middle e outras vulnerabilidades comuns. As organizações não precisam adquirir complementos caros e podem integrar o MaaS360 com suas aplicações de segurança existentes para ajudar a manter o custo total de propriedade no nível desejado.

Por que escolher a IBM?
O IBM Security MaaS360 with Watson possui recursos avançados de segurança para endpoints, aplicações e conteúdo, abrangendo essencialmente os principais sistemas operacionais e tipos de dispositivos. O MaaS360 apresenta IA e análise de segurança, prevenção de perda de dados, gerenciamento de ameaças móveis e gerenciamento de identidade e acesso, permitindo políticas e regras de conformidade enquanto ajuda as empresas a estabelecer uma abordagem de zero trust para sua estrutura de segurança.

Para obter mais informações
Para saber mais sobre o IBM Security MaaS360 with Watson, fale com um representante da IBM ou Parceiro de Negócios IBM ou acesse ibm.com/br-pt/products/unified-endpoint-management.

Notas
1. Relatório de 2022: O custo de uma violação de dados, IBM, julho de 2022
2. Pesquisa de gerenciamento e segurança do espaço de trabalho corporativo dos EUA, 2021: destaques e tendências do gerenciamento de dispositivos de endpoint, IDC, agosto de 2021

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo – SP Brasil.
Produzido nos
Estados Unidos da América,
outubro de 2022