PROPOSTA DE PREÇOS

Ref.: Pregão Eletrônico SRP Nº 08/2022 (UASG 927.131)

À

PRODAM – Processamento de Dados Amazonas S.A,

Prezado Pregoeiro,

Senhor Gilson de Sena da Silva

A empresa **5 Instituto Tecnológico – Sociedade Civil de Profissionais de Tecnologia Associados**, por meio de seu representante legal, vem através deste documento apresentar sua proposta comercial para "*eventual Aquisição de solução de cibersegurança, auditoria e prevenção de ameaças à base de dados não estruturados em endpoint, na modalidade de subscrição, incluindo garantia, serviço de instalação e treinamento*" para atender às necessidades da **PRODAM – Processamento de Dados Amazonas S.A**, conforme especificações detalhadas no Termo de Referência, constante do Anexo I, do edital do Pregão Eletrônico nº **08/2022** deste órgão:

GRUPO	ITEM	ESPECIFICAÇÃO	Referência	QTD.	Valor Unitário (R$)	Valor Total (R$)
1	1	Solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, em endpoint	Licença de uso	15.000	R$ 795,00	R$11.925.000,00
	2	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaça à base de dados não estruturados em endpoint	Serviço	2	R$25.000,00	R$ 50.000,00
	3	Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados em endpoint	Turma	4	R$15.000,00	R$ 60.000,00
VALOR TOTAL DA PROPOSTA (R$)						**R$12.035.000,00**

(Valor por extenso: Doze milhões e trinta e cinco mil reais)

Importantes Considerações e Declarações:

Ao efetuar essa proposta, esta empresa proponente declara que:

- Os produtos ofertados atendem rigorosamente as especificações descritas no Termo de Referência, anexo do Edital Nº 08/2022;
- Está ciente e concorda com as condições contidas no edital Nº 08/2022 e seus anexos;
- Cumpre os requisitos para a habilitação definidos no edital Nº 08/2022 e que a proposta apresentada está em conformidade com as exigências editalícias;
- Nos valores propostos já estão inclusas todas as despesas necessárias para o cumprimento da obrigação contratual, cobrindo todos os custos operacionais, fretes, tarifas, tributos, encargos sociais, encargos trabalhistas, encargos previdenciários, comerciais, lucros, encargos fiscais e para-fiscais, despesas diretas e indiretas e demais despesas decorrentes da execução do objeto do referido edital; e
- Esta proposta tem validade de 90 (noventa) dias corridos a contar da data de sua apresentação.

Comprovação da Boa Situação Financeira da Empresa:

Apresentamos a seguir, os índices que comprovam a boa situação financeira da empresa **5 Instituto Tecnológico – Sociedade Civil de Profissionais de Tecnologia Associados** através dos índices extraídos do Balanço 2021 (documento "03-5IT - Balanço Patrimonial (2021).pdf", em anexo) conforme solicitado no referido edital:

Dados do Balanço		
Ativo Total	R$	1.283.092,35
Ativo Circulante	R$	586.986,99
Ativo Realizável LP	R$	12.948,15
Passivo Circulante	R$	18.290,25
Passivo Não Circulante	R$	22.102,28
Passivo Exigível a LP	R$	22.108,28

Valor da Proposta	R$	12.035.000,00

Índices Exigidos no Edital (maior que 1)		
Liquidez Geral (LG)	14,85	ok
Solvência Geral (SG)	31,77	ok
Liquidez Corrente (LC)	32,09	ok

Patrimônio Líquido Mínimo Exigido (10%)		
Patrimônio Líquido	R$ 1.229.751,67	10,22%

Todos os demais documentos que comprovam os índices apresentados acima foram anexados no sistema ComprasNet (Endereço Eletrônico: https://www.gov.br/compras) juntamente com esta proposta comercial. São eles:

- "03-5IT - Balanço Patrimonial (2021).pdf";
- "04-5IT - Termo de Abertura e Encerramento (2021) .pdf";
- "05-5IT - DRE (2021) .pdf";
- "06-5IT - Recibo ECD 2022.pdf";
- "07-5IT - Análise Econômico-Financeira (2021) .pdf";
- "08-5IT - Certidão Habilitação CRC.pdf"; e
- "09-5IT - Certidão Regularidade CRC.pdf";

Nossas Informações Comerciais

Razão Social	5 INSTITUTO TECNOLOGICO - SOCIEDADE CIVIL DE PROFISSIONAIS DE TECNOLOGIA ASSOCIADOS
CNPJ	27.685.014/0001-42
Endereço	SCN Quadra 02, Bloco D, Loja 310, Shopping Liberty Mall
Bairro	Asa Norte
Cidade	Brasília
Estado	Distrito Federal
CEP	70.712-904
Site	www.5it.com.br/
Telefone	(61) 98138-8139
Contato	Edmundo Pinheiro Germano Braga
E-mail	edmundo@5IT.com.br

Nosso Representante Legal

Nome	Edmundo Pinheiro Germano Braga
Cargo	Presidente
CPF	385.311.511-04
RG	989.289 SESPDF
Endereço	SCN Quadra 02, Bloco D, Loja 310, Shopping Liberty Mall
Bairro	Asa Norte
Cidade	Brasília
Estado	Distrito Federal
CEP	70.712-904

Nossas Informações Bancárias

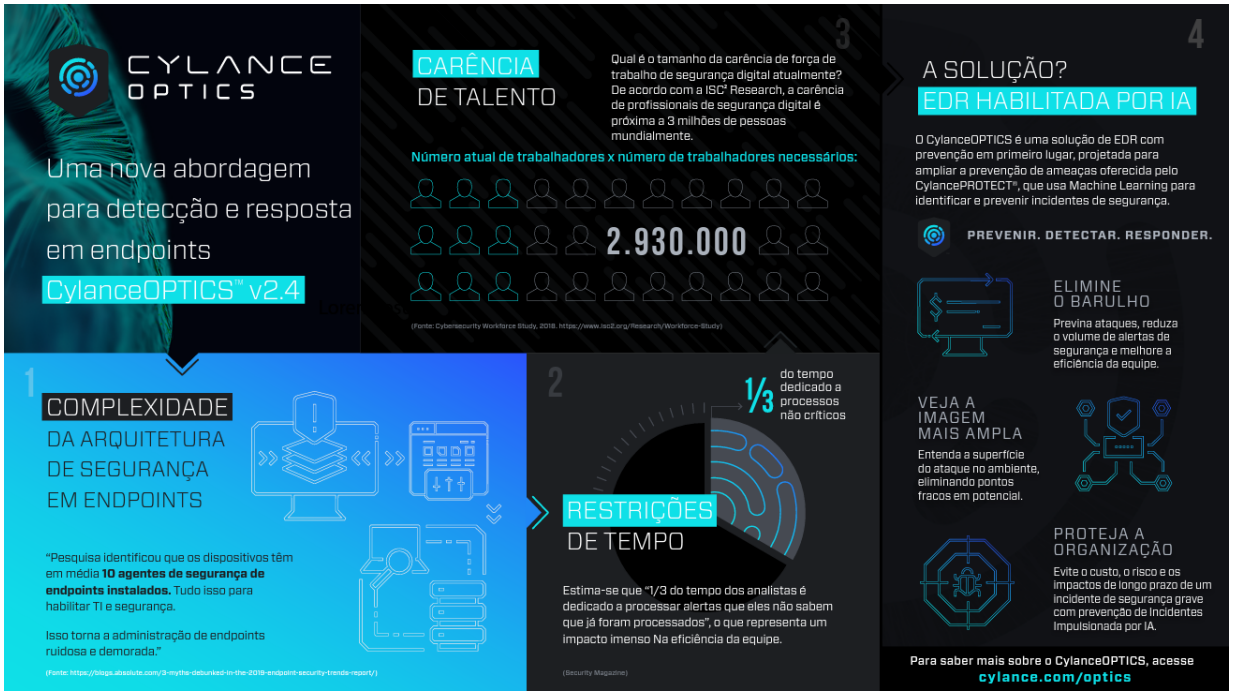
Banco	SICOOB – 756
Agência	4364
Conta corrente	30.168-0

Brasília, 17 de outubro de 2022.

5 Instituto Tecnológico
CNPJ: 27.685.014/0001-42
Edmundo Pinheiro Germano Braga
Representante Legal

Descrição e Características Principais do Objeto Ofertado

- Solução ofertada para o item nr. 1 (Solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, em endpoint), conforme quantidades e exigências estabelecidas no edital:
  - PO.LA.STD.SD.AD – BlackBerry Protect + Optics – Devices – Gov - Support (5000 +)



Declaração de Inexistência de Fatos Impeditivos

O **5 Instituto Tecnológico Sociedade Civil de Profissionais de Tecnologia Associados**, inscrito no C.N.P.J. sob o nº 27.685.014/0001-42, sediada no Setor Comercial Norte, Quadra 02, Bloco D, Loja 310, Shopping Liberty Mall, em Brasília, DF, CEP 70.712-904, **DECLARA**, que até a presente data inexistem fatos impeditivos de sua habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores.

Brasília, 17 de outubro de 2022.

5 Instituto Tecnológico
CNPJ: 27.685.014/0001-42
Edmundo Pinheiro Germano Braga
Representante Legal

Declaração Relativa à Trabalho de Menores, Trabalho Degradante ou Forçado

O **5 Instituto Tecnológico Sociedade Civil de Profissionais de Tecnologia Associados**, inscrito no C.N.P.J. sob o nº 27.685.014/0001-42, sediada no Setor Comercial Norte, Quadra 02, Bloco D, Loja 310, Shopping Liberty Mall, em Brasília, DF, CEP 70.712-904 por intermédio de seu representante legal o Sr. Edmundo Pinheiro Germano Braga, portador da Carteira de Identidade nº 989.289 SESPDF e inscrito no C.P.F. sob o nº 385.311.511-04, **DECLARA** para fins de licitação junto à **PRODAM – Processamento de Dados Amazonas S.A** e sob as penas da lei, que não possuímos, em nosso Quadro de Pessoal, empregados menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e em qualquer trabalho, menores de 16 (dezesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos, em observância ao artigo 7º, inciso XXXIII, da Constituição Federal.

Por fim, declaramos que esta empresa não possui em sua cadeia produtiva empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal.

Brasília, 17 de outubro de 2022.

5 Instituto Tecnológico
CNPJ: 27.685.014/0001-42
Edmundo Pinheiro Germano Braga
Representante Legal

Declaração de Elaboração Independente de Proposta

O **5 Instituto Tecnológico Sociedade Civil de Profissionais de Tecnologia Associados**, inscrito no C.N.P.J. sob o nº 27.685.014/0001-42, sediada no Setor Comercial Norte, Quadra 02, Bloco D, Loja 310, Shopping Liberty Mall, em Brasília, DF, CEP 70.712-904 por intermédio de seu representante legal o Sr. Edmundo Pinheiro Germano Braga, portador da Carteira de Identidade nº 989.289 SESPDF e inscrito no C.P.F. sob o nº 385.311.511-04, **DECLARA** para fins de licitação junto ao **PRODAM – Processamento de Dados Amazonas S.A** e sob as penas da lei, que:

1) A proposta apresentada para participar do Pregão Eletrônico nº **08/2022** foi elaborada de maneira independente, e o conteúdo da proposta não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou de fato do referido processo licitatório, por qualquer meio ou por qualquer pessoa;
2) A intenção de apresentar a proposta elaborada para participar do Pregão Eletrônico nº **08/2022** não foi informada, discutida ou recebida de qualquer outro participante potencial ou de fato do Pregão Eletrônico nº **08/2022**, por qualquer meio ou por qualquer pessoa;
3) Que não tentou, por qualquer meio ou por qualquer pessoa, influir na decisão de qualquer outro participante potencial ou de fato do Pregão Eletrônico nº **08/2022** quanto a participar ou não da referida licitação;
4) Que o conteúdo da proposta apresentada para participar do Pregão Eletrônico nº **08/2022** não será, no todo ou em parte, direta ou indiretamente, comunicado ou discutido com qualquer outro participante potencial ou de fato do Pregão Eletrônico nº **08/2022** antes da adjudicação do objeto do referido processo licitatório;
5) Que o conteúdo da proposta apresentada para participar do Pregão Eletrônico nº **08/2022** não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer integrante do **PRODAM – Processamento de Dados Amazonas S.A** antes da abertura oficial das propostas; e
6) Que está plenamente ciente do teor e da extensão desta declaração e que detém plenos poderes e informações para firmá-la.

Brasília, 17 de outubro de 2022.

5 Instituto Tecnológico
CNPJ: 27.685.014/0001-42
Edmundo Pinheiro Germano Braga
Representante Legal

ATESTADO DE CAPACIDADE TÉCNICA

A **COOPCONTA CONTABILIDADE EIRELI**, com sede Rua 34 Norte, Lote 04, Lojas 05 a 10 – Edifício Real Flat, ´Águas Claras, Distrito Federal, inscrita no CNPJ/MF sob o nº. 24.168.459/0001-67, **ATESTA** para os devidos fins de direito, que a empresa **5 Instituto Tecnológico – Sociedade Civil de Profissionais de Tecnologia Associados**, com sede no Setor Comercial Norte, Quadra 02, Bloco "D", loja 310, 1º pavimento, Shopping Liberty Mall, Bairro Asa Norte, Brasília/DF, CEP: 70.712-904, inscrita no CNPJ/MF sob o nº. 27.685.014/0001-42, através do contrato nº. 02/2018, firmado em 05/01/2018, presta serviços para segurança de Servidores e Endpoints compreendendo o fornecimento de Hardware, Software, e Suporte Técnico para esta empresa, conforme a seguir:

1 – DO OBJETO CONTRATUAL

O objeto do referido CONTRATO é a prestação, pela **5IT** à **COOPCONTA**, do Serviço Segurança das informações contemplando Antivírus com EDR e APT com Análise de vulnerabilidades, o qual consiste na proteção do ambiente, dispositivos móveis e aplicações indicadas pela **COOPCONTA** bem como a instalação, suporte 5x8 (1º , 2º e 3º nível) e treinamento para todos os dispositivos indicados.

2 – DA VIGÊNCIA

O Contrato tem o período de vigência de 36 (trinta e seis meses), com data de início firmada em 05/01/2018 e data de término prevista para 04/01/2021.

3 – DAS CARACTERISTICAS DO SERVIÇO CONTRATADO E QUANTITATIVOS

3.1 – Características dos serviços prestados:

- Serviço **ANÁLISE DE VULNERABILIDADES**, o qual consiste no rastreamento de vulnerabilidades nos dispositivos e aplicações da Coopconta;
- Serviço de **INSTALAÇÃO DE ANTIVÍRUS**, com os módulos de EDR e APT, o qual consiste em instalar software de antivírus em todos os dispositivos de interesse da Coopconta em Sistemas servidores Windows e Linux, clientes Windows, Mac, Linux e mobile Android;
- **Ambiente de Rede:** Todo o ambiente tecnológico da Coopconta e de seus clientes/parceiros.

3.2 – Quantitativos:

PLATAFORMA	LOCAL/SITE	GERÊNCIA	QTDE. DESKTOPS	QTDE. SERVIDORES	QTDE. TOTAL
SOPHOS	COOPCONTA	PREMIUM	498	25	523
SOPHOS	COPERATIVA DE TRABALHO DE RECICLAGEM E PRODUÇÃO - CORTRAP		150	3	153
SOPHOS	COOPERATIVA DE TRABALHO DOS CATADORES - RECICLA		71	2	73
SOPHOS	PLANALTO COOPERATIVA AMBIENTAL		30	2	32
SOPHOS	COORACE		75	5	80
SOPHOS	COOPTIVA		16	3	19
SOPHOS	COOPERATIVA DE COLETA SELETIVA DE MATERIAIS RECICLÁVEIS E RESÍDUOS SÓLIDOS RENASCER		98	1	99
SOPHOS	COOPERATIVA RECICLO		145	5	150
SOPHOS	COOPERATIVA DE RECICLAGEM AMBIENTAL PLASFERRO		173	2	175
SOPHOS	COOPERATIVA DE MATERIAL RECICLADO E DE EDUCAÇÃO AMBIENTAL NOVA ESPERANÇA		51	8	59
SOPHOS	COOPERATIVA DE TRABALHO DE RECICLAGEM AMBIENTAL CONSTRUIR		286	7	293
TOTAIS			**1.593**	**63**	**1.656**

Não havendo fatos supervenientes que desabonem a sua conduta técnica e comercial, uma vez que cumpriu com sua obrigação, não havendo reclamação ou objeção quanto à prazo de entrega e qualidade dos produtos/serviços prestados, emitimos o presente atestado.

Brasília, 30 de janeiro de 2020.

ALESSANDRO LUIZ VIANA DA SILVA:48016934153

Assinado de forma digital por ALESSANDRO LUIZ VIANA DA SILVA:48016934153
Dados: 2022.10.14 19:08:00 -03'00'

ALESSANDRO LUIZ VIANA DA SILVA
DIRETOR GERAL
COOPCONTA CONTABILIDADE EIRELI
alessandro@coopconta.com.br

São Paulo, 14 de Outubro de 2022

À
PRODAM – Processamento de Dados Amazonas S.A.

DECLARAÇÃO DE PARCERIA

Em atendimento ao edital do Pregão Eletrônico nº 08/2022 da **PRODAM – Processamento de Dados Amazonas S.A.,** e para fins de prova junto à esta comissão de licitação, declaramos que a empresa **5 Instituto Tecnológico – Sociedade Civil de Profissionais de Tecnologia Associados**, inscrita no CNPJ nº 27.685.014/0001-42, situada na no Setor Comercial Norte, Quadra 02, Bloco D, Loja 310, Shopping Liberty Mall, em Brasília, DF, CEP 70.712-904, é parceira credenciada da **BlackBerry**, estando apta e autorizada a revender, instalar, configurar, dar treinamento, prestar suporte técnico e dar garantia nas condições, localidades e atendimento nos termos do referido edital para as soluções/serviços referentes à contratação dos itens de nº 1, 2 e 3, constantes do referido edital deste órgão.

Fabricante da solução: BlackBerry
Modelo da solução ofertada: CylancePROTECT + OPTICS
Versão: Device - Standard - Advantage Support

Sem mais para o momento,

Walter Mota
Territory Manager –Brazil

BlackBerry Spark Division
+ 5511 94119.1974

+1 954 439 5439
wmota@blackberry.com

BlackBerry Intelligent Security. Everywhere.

BLACKBERRY OPTICS

Detecção e resposta de endpoints com IA, habilitadas pela nuvem e não dependentes da nuvem

DESCRITIVO DE PRODUTO

Em um mundo perfeito, os endpoints seriam inexpugnáveis, os usuários seriam imunes a golpes de phishing e os sistemas vulneráveis sempre seriam corrigidos imediatamente. No mundo real, porém, as organizações prudentes se preparam para a quase certeza de uma violação implementando o BlackBerry® Optics, a solução BlackBerry® Cyber Suite para detecção e resposta de endpoints (EDR) de última geração.

O BlackBerry Optics habilita os analistas de centros de operações de segurança (SOC) a detectar indícios iniciais de uma violação, para que respostas de contenção possam ser iniciadas rapidamente a fim de minimizar os danos. A redução do tempo de resposta não é apenas essencial para a resiliência operacional: também beneficia os resultados da empresa. As organizações que solucionam incidentes em menos de 200 dias obtêm economias de custos médias de US$ 1,12 milhão[2]. O BlackBerry Optics também equipa os analistas com as ferramentas de busca de ameaças e análise de causas raiz de que precisam para diferenciar os sinais sutis de uma ameaça e o ruído aleatório das atividades de rotina.

[1] IBM Security Cost of a Data Breach Report 2020

A ABORDAGEM DE PRÓXIMA GERAÇÃO DA BLACKBERRY PARA EDR

A abordagem da BlackBerry para EDR baseia-se em três pilares:

- **Arquitetura habilitada para a nuvem:** O BlackBerry Optics aplica toda a lógica de detecção e resposta no endpoint, e armazena os dados resultantes de telemetria, alertas e forenses na nuvem para análise offline.
- **Inteligência artificial na borda:** Regras de detecção de ameaças habilitadas por inteligência artificial (IA), aprendizado de máquina (AM) e orientadas por contexto identificam violações de segurança e acionam respostas automáticas que reduzem o tempo médio para detecção (MTTD) e o tempo médio para correção (MTTR).
- **Insight profundo:** O BlackBerry Optics facilita a busca de ameaças e a análise de causas raiz, fornecendo aos analistas acesso contínuo a dados de endpoints correlacionados e contextualizados.

ARQUITETURA HABILITADA PARA A NUVEM

Diferente de outros produtos de EDR, o BlackBerry Optics implementa toda a lógica de detecção e resposta a ameaças no endpoint. Os dados de alertas, eventos e telemetria para os endpoints protegidos são automaticamente coletados, correlacionados e armazenados na nuvem para análise offline. Direto da caixa, os clientes recebem 30 dias de armazenamento na nuvem. A BlackBerry também oferece pacotes de retenção por 90 dias e 365 dias para clientes em setores altamente regulados que precisam de dados históricos adicionais para demonstrar conformidade.

DETECÇÃO DE AMEAÇAS COM IA DE BORDA E ANÁLISE CONTEXTUAL

O Context Analysis Engine (CAE) do BlackBerry Optics monitora eventos de endpoint com velocidade de máquina para identificar atividades maliciosas e suspeitas. O CAE inclui um conjunto predefinido de lógica de detecção com curadoria da BlackBerry, que pode acionar diversas respostas ad-hoc e automáticas. O CAE inclui regras:

- Baseadas em feeds de inteligência de ameaças e relatórios de gerenciamento do setor.
- Derivadas de ataques do mundo real investigados e solucionados em campo pelas equipes de resposta a incidentes e os pesquisadores de ameaças da BlackBerry.
- Mapeadas para a MITRE ATT&CK® Framework.
- Isso alavanca telemetria de CPU exclusiva da Intel® Threat Detection Technology para detectar e mitigar cryptojacking em sistemas operacionais Windows® 10.

PROTEÇÃO DE PRÓXIMA GERAÇÃO

O BlackBerry Optics utiliza IA, AM e análise contextual para:

- Detecção de ameaças
- Busca de ameaças
- Análise de causas raiz
- Acionamento de respostas automáticas para contenção e correção

BENEFÍCIOS

- Utiliza várias técnicas para detectar ataques em estágio inicial.
- Implementa lógica de detecção e resposta no endpoint para minimizar a latência de resposta. Elimina a dependência de pesquisas e conectividade de nuvem.
- Direto da caixa, fornece 30 dias de armazenamento de dados de endpoints na nuvem. Pacotes de retenção mais longos estão disponíveis.
- Roteiros automatizados aceleram a resposta, a correção e a recuperação de incidentes.
- As pesquisas avançadas do InstaQuery facilitam a busca de ameaças e a análise de causas raiz.
- Suporte abrangente para várias plataformas, incluindo Linux®.

O BlackBerry Optics também inclui módulos de detecção de ameaças com aprendizado de máquina desenvolvidos pela equipe de Ciência de Dados da BlackBerry, que analisam continuamente a atividade nos endpoints para detectar ataques de dia zero e ameaças persistentes avançadas (APTs). Os analistas do SOC também podem criar regras personalizadas que refletem as políticas de segurança específicas do ambiente de sua organização.

RESPONDENDO A AMEAÇAS COM PACOTES SOB DEMANDA E ROTEIROS AUTOMÁTICOS

O BlackBerry Optics fornece respostas sob demanda e automáticas sempre que uma regra de detecção é acionada.

- **Respostas sob demanda com pacotes:** Os analistas podem usar o mecanismo avançado de criptografia no BlackBerry Optics para criar e implementar pacotes. Os pacotes são conjuntos de scripts executados no endpoint para acionar aplicativos, coletar dados forenses, desativar sistemas e executar outras funções de investigação e correção. Podem ser implementados sob demanda para um único dispositivo, vários dispositivos, zonas de segurança selecionadas ou em toda a empresa.
- **Respostas automáticas com roteiros:** Os pacotes também podem ser combinados e configurados como roteiros que são executados automaticamente quando uma regra de detecção é acionada. Por exemplo, um analista pode criar um roteiro que coleta automaticamente registros do PowerShell, arquivos de histórico de navegação e dados

de dump de memória sempre que um endpoint executa um comando do PowerShell para fazer download de um arquivo.

BUSCA DE INDICADORES DE COMPROMETIMENTO COM CONSULTAS AVANÇADAS DO INSTAQUERY

O BlackBerry Optics simplifica a busca de ameaças, habilitando as equipes de segurança a coletar e analisar dados usando consultas avançadas do InstaQuery (IQ). O IQ é uma ferramenta leve que coleta e agrega dados relevantes de endpoints e os apresenta em um formato contextualizado e com análise intuitiva. Permite que os analistas respondam a perguntas como:

- Este valor de hash ou esta extensão de arquivo já foram vistos em um de meus endpoints antes?
- Esta linha de comando já foi executada em um de meus sistemas?

CASOS COMUNS DE USO DO BLACKBERRY OPTICS

O BlackBerry Optics é adequado para organizações que desejam:

- Reduzir MTTD e MTTR, contendo as ameaças com pacotes sob demanda e roteiros automáticos.
- Corrigir ameaças restaurando rapidamente os sistemas comprometidos de volta a um estado inalterado.
- Pesquisar dados de endpoint para identificar arquivos, executáveis, objetos MITRE ATT&CK e outros indicadores de comprometimento.
- Proteger os endpoints sem gargalos de desempenho.
- Identificar rapidamente os sinais de um ataque ocultos em grandes quantidades de dados de endpoints.
- Aumentar a resiliência, dinamizando a busca de ameaças e a análise de causas raiz.

PARA MAIS INFORMAÇÕES

Saiba mais sobre o BlackBerry Optics e o BlackBerry Cyber Suite.

BlackBerry. Intelligent Security. Everywhere.

A BlackBerry (NYSE: BB; TSX: BB) fornece softwares e serviços de segurança inteligentes para empresas e governos no mundo inteiro. A empresa protege mais de 500 milhões de endpoints, incluindo 175 milhões de carros em circulação atualmente. Sediada em Waterloo, Ontário, Canadá, a empresa alavanca IA e aprendizado de máquina para entregar soluções inovadoras nas áreas de segurança digital, proteção e privacidade de dados, e é líder em gerenciamento de segurança de endpoints, criptografia e sistemas incorporados. A visão da BlackBerry é clara — proteger um futuro conectado em que você pode confiar.

*Para obter mais informações, acesse **BlackBerry.com** e siga **@BlackBerry**.*

BlackBerry Intelligent Security. Everywhere.

MITIGANDO INCIDENTES EM MILISSEGUNDOS

com detecção e resposta em endpoints habilitadas por IA.

RESUMO DA SOLUÇÃO

INTRODUÇÃO

A época em que uma organização podia fortalecer seu perímetro de rede para reduzir os riscos cibernéticos acabou. A proliferação de dispositivos móveis e IoT que compartilham dados e se conectam com várias redes criou uma superfície de ataque que se expande exponencialmente.

Nesse novo ambiente de ameaças, a principal prioridade é prevenir que os adversários infectem esses dispositivos de longo alcance com malware. O BlackBerry® Protect, plataforma de proteção de endpoints da BlackBerry®, realiza isso com tecnologias de inteligência artificial (IA) e aprendizado de máquina (AM) que previnem a detonação de formas conhecidas e desconhecidas de malware.

Como a Verizon observou[1], no entanto, "O malware tem estado em declínio consistente e constante como porcentagem das violações nos últimos 5 anos". Isso não significa que o malware está desaparecendo como um vetor de ataque. Quer dizer apenas que os adversários estão aumentando o uso de TTPs que não requerem o uso de executáveis portáteis para comprometer um endpoint. Por exemplo, estão usando phishing para furtar credenciais de usuário, explorando vulnerabilidades amplamente conhecidas em serviços de rede com uso externo, como RDP, e incorporando backdoors em aplicativos amplamente usados, como nos ataques à SolarWinds.

[1] Relatório de Investigações sobre Violações de Dados de 2020

Essas táticas com frequência envolvem uma sequência de atividades aparentemente benignas que somente em combinação revelam sua intenção maliciosa. Um ponto de dados individual só pode ser significativo com base no contexto em que aparece e sua correlação com outros eventos de segurança.

Esse tipo de análise contextual é muito compatível com soluções de detecção e resposta em endpoints (EDR).

Assim, o EDR tem potencial para exercer dois papéis essenciais na defesa cibernética. Em primeiro lugar, pode alertar os analistas de centros de operações de segurança (SOC) quando detecta indícios iniciais de uma violação de segurança, para que respostas de contenção possam ser iniciadas com rapidez suficiente para minimizar os danos. A redução do tempo de resposta não é apenas essencial para a resiliência operacional: também beneficia os resultados da empresa. As organizações que solucionam incidentes em menos de 200 dias obtêm economias de custos médias de US$ 1,12 milhão[2].

A segunda função é equipar os analistas com os dados de que precisam para buscar proativamente as ameaças e fazer análise de causas raiz após o incidente. No entanto, considerando a proliferação de dispositivos de endpoint, e os volumes imensos de dados de telemetria e eventos que geram, como um analista pode diferenciar os indícios sutis de ameaças e os ruídos aleatórios das atividades de rotina?

Neste resumo de solução, vamos considerar como a solução EDR habilitada por IA da BlackBerry, o BlackBerry® Optics, é excelente para ajudar os clientes a alcançar esses dois objetivos. Por exemplo, depois de implementar BlackBerry Protect e BlackBerry Optics, um cliente[3]:

- **Reduziu o tempo perdido em 95%** com investigação e correção mais rápidas: Menos usuários finais foram comprometidos. A maior rapidez para investigação e correção de ameaças permitiu que os usuários finais reiniciassem o trabalho produtivo rapidamente.
- **Redução de 97% nas reimagens de máquinas**: Isso permitiu que o cliente realocasse recursos de TI para projetos mais produtivos.
- **Economia de US$ 8,4 milhões** (valor presente líquido) com a desativação das soluções de segurança de endpoints legadas da empresa.

ABORDAGEM DA BLACKBERRY PARA EDR

A abordagem de próxima geração da BlackBerry para EDR baseia-se em três pilares:

- **Arquitetura habilitada para a nuvem**: O BlackBerry Optics aplica toda a lógica de detecção e resposta no endpoint, e armazena os dados resultantes de telemetria, alertas e forenses na nuvem para análise off-line.
- **Inteligência Artificial na Borda**: Regras de detecção de ameaças habilitadas por IA e orientadas por contexto identificam violações de segurança e acionam respostas automáticas que reduzem o tempo médio para detecção (MTTD) e o tempo médio para correção (MTTR).
- **Insight Profundo**: O BlackBerry Optics facilita a busca de ameaças e a análise de causas raiz, fornecendo aos analistas uma visão consolidada, correlacionada, orientada por IA e para toda a empresa das atividades históricas nos endpoints.

[2] Relatório de Custos de Segurança por Violação de Dados da IBM de 2020

[3] Estudo Total Economic Impact™ da Forrester

ARQUITETURA HABILITADA PARA A NUVEM

Diferente de outros produtos de EDR, o BlackBerry Optics implementa toda a lógica de detecção e resposta a ameaças no endpoint. Na prática, cada endpoint funciona como um SOC autônomo, detectando e respondendo a ameaças em tempo quase real, sem depender de conectividade com a nuvem. Isso elimina a latência de resposta que permite que um evento de segurança secundário se transforme em um incidente de segurança de grande porte.

Os dados de alertas, eventos e telemetria para todos os endpoints protegidos são automaticamente coletados, correlacionados e armazenados na nuvem para análise off-line. Direto da caixa, os clientes recebem 30 dias de armazenamento na nuvem. A BlackBerry também oferece opções de pacotes de retenção por 90 dias e 365 dias para clientes em setores altamente regulados que precisam de dados históricos adicionais para demonstrar conformidade. Essa abordagem de nuvem híbrida elimina as limitações de armazenamento físico no endpoint, e garante flexibilidade máxima para busca de ameaças e análise após incidentes.

IA NA BORDA

O termo IA na Borda refere-se à prática da BlackBerry de implementar tecnologias sofisticadas de inteligência artificial e aprendizado de máquina no endpoint para reduzir os riscos cibernéticos. A IA na Borda é encontrada em BlackBerry Protect, BlackBerry Optics e BlackBerry® Persona.

Detecção de ameaças com o Context Analysis Engine

O Context Analysis Engine (CAE) do BlackBerry Optics é incorporado em cada endpoint, monitorando eventos com velocidade de máquina para identificar atividades maliciosas e suspeitas. O CAE inclui um conjunto predefinido de lógica de detecção com curadoria da BlackBerry, que pode acionar diversas respostas ad-hoc e automáticas. O CAE inclui regras:

- Baseadas em feeds de inteligência de ameaças e relatórios de gerenciamento do setor.
- Derivadas de ataques do mundo real investigados e solucionados em campo pelas equipes de resposta a incidentes da BlackBerry, e também ataques desconstruídos e documentados por pesquisadores de ameaças da BlackBerry. Por exemplo, a equipe de Resposta a Ameaças da BlackBerry criou regras personalizadas que protegem os clientes contra ataques do Hafnium em servidores Microsoft Exchange vulneráveis, e outras que identificam e mitigam variantes do ransomware Ryuk .
- Criadas por analistas de SOC que refletem políticas de segurança específicas do ambiente. Por exemplo, um analista pode definir uma regra que aciona uma coleta de dados de alertas e forenses sempre que um usuário final tentar acessar um recurso restrito ou aumentar seus privilégios de conta.
- Mapeadas para a MITRE ATT&CK® Framework, um banco dados de conhecimentos global com táticas e técnicas de agentes de ameaças obtidas em ataques cibernéticos do mundo real.
- Isso alavanca telemetria de CPU exclusiva da Intel® Threat Detection Technology para detectar e mitigar cryptojacking em sistemas operacionais Windows® 10. As regras de cryptojacking podem ser configuradas facilmente e praticamente não têm impacto no processador dos sistemas protegidos.

Embora as regras de detecção sejam necessárias, não podem modelar todos os tipos de comportamentos de ataque. Portanto, o BlackBerry Optics também inclui módulos de detecção de ameaças com aprendizado de máquina desenvolvidos pela equipe de Ciência de Dados da BlackBerry, que analisam continuamente a atividade nos endpoints para detectar ataques de dia zero e ameaças persistentes avançadas (APTs).

Respondendo a ameaças com pacotes sob demanda e roteiros automáticos

O BlackBerry Optics fornece respostas sob demanda e automáticas sempre que uma regra de detecção do CAE ou de aprendizado de máquina é acionada. Ambos são essenciais para minimizar o tempo de permanência e reduzir custos, riscos e impactos de longo prazo resultantes de um incidente de segurança abrangente.

- **Respostas sob demanda com pacotes:** Os analistas podem usar o mecanismo avançado de criptografia no BlackBerry Optics para criar e implementar pacotes. São conjuntos de scripts executados no endpoint para acionar aplicativos, coletar dados forenses, desativar sistemas e executar outras funções de investigação e correção. O BlackBerry Optics é entregue com um conjunto padrão de pacotes para muitas tarefas de rotina. Os pacotes podem ser implementados sob demanda e em escala para um único dispositivo, vários dispositivos, zonas de segurança selecionadas ou em toda a empresa.
- **Respostas automáticas com roteiros:** Os pacotes também podem ser combinados e configurados como roteiros, conjuntos complexos de ações de resposta que são executadas automaticamente quando uma detecção do CAE ou de aprendizado de máquina é acionada. Por exemplo, um analista pode criar um roteiro de coleta de dados forenses que é executado sempre que um endpoint executa um comando do PowerShell para fazer download de um arquivo. Quando a regra é acionada, o roteiro pode coletar automaticamente os registros do PowerShell, arquivos de histórico de navegação e dados de um dump de memória, fornecendo informações forenses contextualizadas para o analista sem necessidade de uma única ação no teclado.

INSIGHT PROFUNDO

Depois que um incidente é detectado, deve ser investigado de forma abrangente para garantir que todos os estágios da cadeia de ataque sejam entendidos e considerados em esforços posteriores de contenção e recuperação. O termo Insight Profundo refere-se ao conjunto abrangente de ferramentas manuais e automáticas para investigação de incidentes e busca de ameaças, que fornecem aos analistas acesso contínuo aos dados de endpoints.

Busca de indicadores de comprometimento com consultas de InstaQuery

Os caçadores de ameaças usam processos baseados em inteligência e metodologia para identificar eventos de segurança anômalos e padrões de atividade que se combinam para indicar que um ataque pode estar ocorrendo. Isso tradicionalmente exigia analistas de elite, com habilidades especializadas e experiência abrangente. Felizmente, o BlackBerry Optics torna possível que analistas com todos os níveis de habilidades possam buscar ameaças com facilidade e eficiência.

O BlackBerry Optics simplifica o processo de busca de ameaças, habilitando as equipes de segurança a coletar e analisar dados usando consultas avançadas do InstaQuery (IQ). O IQ é uma ferramenta leve que coleta e agrega dados relevantes de endpoints e os apresenta em um formato contextualizado e com análise intuitiva. As consultas do IQ podem coletar artefatos associados com arquivos, chaves de registro, processos, conexões de rede e muito mais. Permite que os analistas respondam a perguntas como:

- Este valor de hash ou esta extensão de arquivo já foram vistos em um de meus endpoints antes?

- Esta linha de comando já foi executada em um de meus sistemas?

Os consultores de Resposta a Incidentes da BlackBerry utilizaram o IQ recentemente para ajudar uma grande empresa a investigar e corrigir um ataque de ransomware. Em segundos, a equipe determinou que o indicador de comprometimento primário, a extensão de arquivo do ransomware, só estava presente nos EUA. Isso habilitou o cliente e as equipes da BlackBerry a concentrar seus esforços de investigação, remediação e limpeza ali, em vez de dedicar horas não produtivas a avaliar os ambientes operacionais do cliente na Europa, na Ásia e no sul do Pacífico. Os consultores da BlackBerry também ajudaram o cliente a prevenir infecções adicionais, criando e distribuindo regras personalizadas que garantiram que o ransomware seria detectado instantaneamente e colocado em quarentena.

Otimizações para ambientes Linux

O BlackBerry Optics também oferece proteção aprimorada para sistemas com versões do sistema operacional Linux®, incluindo RHEL, Ubuntu, CentOS e SUSE. Proteger sistemas Linux é essencial, porque os grupos de APT estão cada vez mais vendo o Linux como um alvo rico em oportunidades. Em um relatório recente, a equipe de Pesquisa e Inteligência da BlackBerry observou que a maioria das empresas de segurança concentra sua atenção de engenharia e marketing em produtos elaborados para o front office e não para os servidores. A cobertura defensiva para Linux com frequência é escassa e imatura. O BlackBerry Optics aborda essas falhas de segurança com recursos específicos para o Linux, que incluem:

- **Uma arquitetura sem drivers** que aumenta a segurança ao eliminar as dependências em nível de kernel.
- **Regras de CAE para Linux** que detectam automaticamente eventos de malware e maliciosos.
- **Refract for Linux**, que corrige automaticamente eventos de malware e maliciosos.
- **Bloqueio de dispositivos**, que facilita a correção e recuperação de incidentes, isolando endpoints infectados para bloquear a disseminação de malware.

Esses recursos permitem que os administradores detectem e bloqueiem ameaças em ataques a servidores de datacenters, dispositivos de ponto de venda (PDV), terminais de caixas automáticos e dispositivos com função fixa baseados em Linux. O Linux também é ubíquo em servidores web, supercomputadores, grandes websites e prestadores de serviços de nuvem, incluindo Google, Yahoo e Amazon.

BENEFÍCIOS ESPERADOS

A abordagem baseada em IA da BlackBerry para EDR ajuda as organizações a reduzir os riscos cibernéticos, ao:

- **Conter ameaças com respostas automáticas**. Isso inclui isolar dispositivos, encerrar processos e adotar outras ações apropriadas que evitam que os agentes de ameaças furtem credenciais, aumentem privilégios, movam-se lateralmente na rede ou concretizem seus objetivos de outras formas.
- **Corrigir ameaças retornando os sistemas afetados de volta a um estado inalterado anterior**. Isso inclui eliminar todos os rastros do ataque, e também seus mecanismos de persistência e artefatos forenses.
- **Ajudar os analistas a identificar os sinais de um ataque** ocultos nas quantidades maciças de dados de telemetria de endpoints históricos e metadados armazenados na nuvem. Isso inclui todos os arquivos criados, todos os processos iniciados, todas as alterações em chaves de registro, todas as conexões de rede, etc. O BlackBerry Optics concretiza isso com regras de detecção automáticas orientadas por IA e análise contextual.
- **Dinamizar o processo de rastrear ataques e identificar falhas de segurança**, fornecendo aos analistas acesso imediato aos dados contextualizados de que precisam para busca eficiente de ameaças e análise de causas raiz.

PARA MAIS INFORMAÇÕES

Saiba mais sobre o BlackBerry Optics e o BlackBerry Cyber Suite.

BlackBerry. Intelligent Security. Everywhere.

A BlackBerry (NYSE: BB; TSX: BB) fornece softwares e serviços de segurança inteligentes para empresas e governos no mundo inteiro. A empresa protege mais de 500 milhões de endpoints, incluindo 175 milhões de carros em circulação atualmente. Sediada em Waterloo, Ontário, Canadá, a empresa alavanca IA e aprendizado de máquina para entregar soluções inovadoras nas áreas de segurança digital, proteção e privacidade de dados, e é líder em gerenciamento de segurança de endpoints, criptografia e sistemas incorporados. A visão da BlackBerry é clara — proteger um futuro conectado em que você pode confiar.

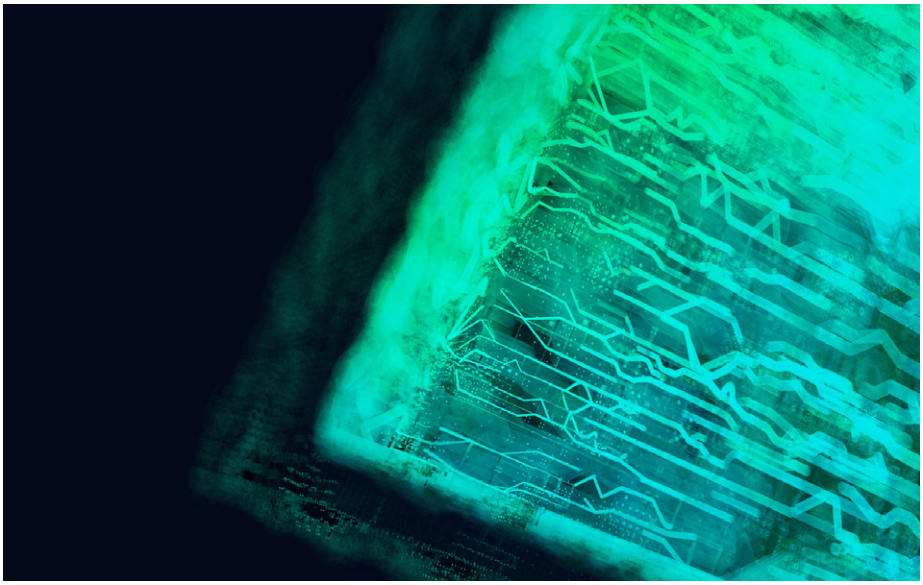
*Para obter mais informações, acesse **BlackBerry.com** e siga **@BlackBerry**.*

BlackBerry
Intelligent Security. Everywhere.

Descritivo de Produto

BlackBerry Protect

Segurança de endpoints à prova de futuro



Há anos, a proteção contra ameaças primária dos produtos de segurança de endpoints baseava-se em assinaturas, criadas depois que pacientes zero eram impactados e o dano já havia ocorrido. Com o pressuposto de que todos os ataques já haviam sido vistos antes, usar assinaturas fazia sentido. Hoje, o malware passa por mutações diariamente, ou até a cada hora, o que torna obsoletas as ferramentas de prevenção com base em assinaturas, e cria a necessidade de uma abordagem mais forte com base em prevenção para a segurança de endpoints.

A BlackBerry redefiniu o que uma solução de proteção de endpoints pode e deve fazer para as organizações, usando uma abordagem automática de prevenção em primeiro lugar. É uma solução precisa, eficiente e eficaz para prevenir a execução de ameaças persistentes avançadas (APTs) e malwares nos endpoints de sua organização. O BlackBerry® Protect previne violações e fornece controles de segurança adicionais para proteger contra ataques baseados em scripts, sem arquivos, de memória e com base em dispositivos externos. O BlackBerry Protect atua sem intervenção de usuário ou administrador, e sem conexão de nuvem, assinaturas, heurísticas ou sandboxes.

Capacidades

Aplicação de Políticas de Uso de Dispositivos

- Controle o uso de dispositivos de armazenamento de massa USB
- Previna o roubo de dados por meio de mídias removíveis

Controles de Acesso com Base em Função (RBAC, Role-Based Access Controls)

- Minimize o risco com administração de funções mais granular usando RBAC personalizado
- Aprimore as restrições para acesso à rede com base nas funções de usuários individuais
- Limite os direitos de acesso de funcionários apenas às informações de que precisam para suas tarefas
- Beneficie-se da ausência de impacto para os usuários atuais

Controle de Aplicativos

- Restringir dispositivos com função fixa
- Previna binários ruins ou modificação de um binário
- Bloqueie sistemas especificados e restrinja alterações

BlackBerry Protect

BlackBerry Protect para Desktop

O modelo algorítmico usado no BlackBerry Protect significa que não há assinaturas, patches, scans de sistema ou endpoints lentos devido à solução de segurança executada neles. Os clientes que migraram de produtos antivírus com base em assinaturas, reativos e tradicionais, observaram um ROI de até 99%, uma redução de 97% na reimagem de máquinas, desempenho estendido de hardware e bateria, e redução de 90% nas horas de pessoal necessárias para administrar a solução.[1]

A arquitetura do BlackBerry Protect consiste em um agente único leve que é administrado pelo console de nuvem SaaS exclusivo da BlackBerry. O console de nuvem integra-se facilmente com sistemas de administração de software e ferramentas de segurança existentes. Opções de administração híbridas e locais estão disponíveis para ambientes air-gapped. O agente de endpoint detecta e previne malware no host, independente de conexão de nuvem e sem necessidade de atualizações contínuas. O BlackBerry Protect tem capacidade para detectar e colocar em quarentena os malwares em redes abertas, isoladas e virtuais. A abordagem de machine learning da BlackBerry impede a execução de código malicioso, sem necessidade de conhecimento anterior ou uso de uma técnica de ofuscação desconhecida. Nenhum outro produto antimalware compara-se à precisão, facilidade de administração e eficácia do BlackBerry Protect.

Características do BlackBerry Protect

Prevenção de Dia Zero Verdadeira

Modelo de IA resiliente previne a execução de payloads de dia zero.

Aplicação de Políticas de Uso de Dispositivos

Controla quais dispositivos podem ser usados no ambiente, eliminando dispositivos externos como um possível vetor de ataque.

Prevenção contra Malwares Impulsionada por IA

IA comprovada em campo inspeciona qualquer aplicativo que tenta se executar em um endpoint, antes que seja executado.

Detecção e Prevenção de Exploits de Memória

Identifica proativamente o uso malicioso de memória (ataques sem arquivos) com respostas de prevenção automáticas e imediatas.

Administração de Scripts

Mantém o controle integral de onde e quando os scripts são executados em seu ambiente.

Controle de Aplicativos para Dispositivos com Função Fixa

Garante que os dispositivos com função fixa estejam em estado inalterado continuamente, eliminando os desvios que ocorrem com dispositivos não administrados.

Capacidades

Proteção de Memória

- Identificar proativamente e impedir o uso malicioso de memória
- Prevenir ataques somente de memória, como encaminhamento de privilégios
- Benefício de exclusões granulares e solução de problemas e relatórios aprimorados

Controle de Scripts

- Impedir a execução de scripts não autorizados
- Benefício de recursos granulares de listas de aprovação e lista de segurança
- Compatível com MacOS®, Microsoft® e Linux®
- Impedir a execução de one-liners PowerShell

Detecção de Aplicativos Sideloaded iOS®

- Os aplicativos sideloaded são detectados e examinados imediatamente

BlackBerry Protect para Dispositivos Móveis

Agora, mais do que nunca, as organizações estão usando dispositivos móveis para competir em um mercado ágil e em evolução, e manter os colaboradores conectados. Pela primeira vez, mais de metade de todos os dispositivos conectados à Internet são móveis[2]. Ao mesmo tempo, o malware móvel é mais prevalente do que nunca, com um aumento de 50% nos ataques apenas no ano passado[3]. Embora o foco das soluções de segurança empresarial historicamente tenha sido em dispositivos de mesa, cada vez mais empresas estão descobrindo a ameaça crescente dos ataques de phishing em dispositivos móveis, especialmente dentro de aplicativos.

Os danos decorrentes desses ataques podem ser significativos, com vazamento de informações de identificação pessoal (PII) e outros dados críticos em taxas mais altas do que nunca antes. Isso está levando mais organizações a adotar inspeção profunda de pacotes (DPI) e outros recursos para proteger contra ataques maliciosos.

Portanto, não surpreende que o mercado de defesa contra ameaças móveis (MTD) esteja crescendo rápido. O MTD oferece uma camada adicional de segurança, prevenindo, detectando, corrigindo e aprimorando a higiene de segurança geral para todos os níveis na frota móvel e nos aplicativos da organização.

Nossa solução de MTD do BlackBerry Protect amplia a linha de base de segurança fornecida pelo BlackBerry® UEM, abordando as ameaças maliciosas avançadas em dispositivos móveis. O BlackBerry Protect monitora ataques em dispositivos e aplicativos, e vai além da segurança dos containers de aplicativos básicos BlackBerry.

- Em nível de dispositivo, o BlackBerry Protect para dispositivos móveis identifica vulnerabilidades de segurança e atividades maliciosas potenciais, monitorando atualizações do SO, parâmetros do sistema, configurações de dispositivos e bibliotecas do sistema.
- Em nível de aplicativos, o BlackBerry Protect para dispositivos móveis usa sandboxing de aplicativos e análise de códigos, e também teste de segurança de aplicativos, para identificar malware e grayware.

Além disso, o BlackBerry Protect para dispositivos móveis identifica qualquer malware que possa vir em aplicativos sideloaded, malware exclusivo baseado em assinaturas, ou simulações, adicionando uma camada extra de segurança à plataforma SDK do BlackBerry Dynamics. Isso permite que parceiros e empresas criem aplicativos personalizados e seguros, que podem ser carregados em dispositivos para acesso das empresas.

Capacidades

Scans de Malware em Android™

Scans de Malware Android e APK na App Store UEM

- Examina todos os aplicativos na app store BlackBerry UEM, incluindo aplicativos personalizados de parceiros e clientes, protegendo contra malware

Detecção de URLs de Phishing e Maliciosos

- Alavanca IA para detectar e impedir automaticamente URLs maliciosos, incluindo aqueles com elementos de phishing incorporados.

Criação de Aplicativos Seguros

- Permite que parceiros e empresas criem aplicativos personalizados e seguros para dispositivos acessados por empresas

Verificação de Integridade de Apps iOS para Apps desenvolvidas com o BlackBerry Dynamics

- Garante a integridade de aplicativos criados na plataforma SDK do BlackBerry® Dynamics™ SDK
- Só permite que aplicativos seguros sejam carregados em dispositivos e previne adulterações de aplicativos BlackBerry®

Casos Comuns de Uso do BlackBerry Protect

O BlackBerry Protect fornece prevenção contra ameaças de espectro completo que impede as violações nos endpoints, solucionando os seguintes casos de uso:

- Identificar e bloquear executáveis maliciosos sem necessidade de atualizações constantes ou uma conexão de nuvem
- Identificar vulnerabilidades de segurança e atividades maliciosas potenciais, monitorando atualizações do SO, parâmetros do sistema, configurações de dispositivos e bibliotecas do sistema
- Controlar onde, como e quem pode executar os scripts
- Administrar o uso de dispositivos USB e impedir que dispositivos não autorizados sejam usados
- Impedir ataques de malware sem arquivos
- Restringir dispositivos com função fixa, como quiosques, terminais de PDV, etc.
- Prevenir ataques de dia zero e ransomware
- Impedir ataques e exploits com base em memória
- Usar sandboxing de aplicativos e análise de códigos, e também teste de segurança de aplicativos, para identificar malware e grayware
- Identificar qualquer malware que possa vir em aplicativos sideloaded, malware exclusivo baseado em assinaturas ou simulações
- Proteção para endpoints quando os usuários estão online ou offline

Saiba mais

O BlackBerry Protect é apenas um produto de uma ampla gama de soluções de segurança de classe mundial da BlackBerry. Saiba mais sobre a nossa seleção completa de suites de segurança que podem fornecer segurança inteligente para a sua organização, em todos os lugares.

Conheça:

BlackBerry Spark® Suite

BlackBerry Spark® Unified Endpoint Security Suite

BlackBerry Spark® Unified Endpoint Management Suite

1 https://www.cylance.com/en-us/company/about-us/our-customers/2019-forrester-tei-report.html#form-anchor

2 https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet

3 https://research.checkpoint.com/cyber-attack-trends-2019-mid-year-report/

Sobre a BlackBerry

A BlackBerry (NYSE: BB; TSX: BB) fornece softwares e serviços inteligentes de segurança para empresas e governos no mundo inteiro. A empresa protege mais de 500 milhões de endpoints, incluindo 150 milhões de carros em circulação atualmente. Sediada em Waterloo, Ontário, Canadá, a empresa alavanca IA e aprendizado de máquina para entregar soluções inovadoras nas áreas de segurança digital, proteção e privacidade de dados, e é líder em gerenciamento de segurança de endpoints, criptografia e sistemas incorporados. A visão da BlackBerry é clara — proteger um futuro conectado em que você pode confiar.

Para obter mais informações, acesse BlackBerry.com e siga @BlackBerry.

BlackBerry
Intelligent Security. Everywhere.

BB20-0250 | 200617