ESTUDO SOBRE SOLUÇÃO TECNOLÓGICA PARA A MITIGAÇÃO DOS RISCOS CIBERNÉTICOS NO SETOR FINANCEIRO

Gustavo Boldrini Custoias[1], Letícia Breda Mendonça[1], Daniela Vieira Cunha[2]

[1]Ciência da Computação, Faculdade de Computação e Informática – Universidade Presbiteriana Mackenzie (UPM)
CEP: 01302-907 – Campus Higienópolis, São Paulo, SP – Brasil

{gustavo-custoias@outlook.com.br, lemendonca97@gmail.com daniela.cunha@mackenzie.br}

Abstract. *The purpose of this paper is to carry out a survey and a comparative study of technological solutions to mitigate cyber-attacks in the scenario of financial institutions through the use of NAC technologies. In the course of this paper, several tools and results of this comparative study were analyzed so that it would be possible to suggest the best tool available in the market to solve this problem, considering the financial sector scenario.*

Keywords: NAC. IoT. Cybersecurity. Financial Institution. Network.

Resumo. Este trabalho tem como proposito realizar um levantamento e um estudo comparativo de soluções tecnológicas para mitigação de ataques cibernéticos no cenário de instituições financeiras, através do uso de tecnologias NAC. No decorrer deste trabalho foram analisadas diferentes ferramentas e apresentados resultados desse estudo comparativo, para que fosse possível sugerir qual a melhor opção de ferramenta disponível no mercado, para solução do problema, tendo em vista o cenário do setor financeiro.

Palavras Chaves: NAC. IoT. Segurança Cibernética. Instituições Financeiras. Redes.

1. INTRODUÇÃO

O crescimento do uso da Internet alterou a forma de comunicação humana e com ela, a quantidade exponencial de dispositivos IoT (*Internet of Things* – em português, Internet das Coisas). Estes dispositivos proporcionam distintos

benefícios aos seus consumidores, seja na utilização de termostatos em *datacenters*; *wearables* para pagamento – conhecidos como "*mobile payments*"; sensores de movimento para *Data Analysis*, entre outros.

No entanto, é necessário observar que junto aos benefícios proporcionados pelo IoT estão os riscos associados à falta da segurança cibernética. É por isso que a busca por soluções para proteger as redes e os dados sigilosos internos tem sido a "falta de sono" de vários *heads* de *Cybersecurity* das organizações.

Dispositivos mal configurados, sem as proteções de segurança adequadas ou sem visibilidade dos técnicos de TI oferecem aos criminosos cibernéticos um "Passe livre" para acesso à rede e a todas as informações privilegiadas da instituição, através de vírus, *malwares*, *ransowares*, etc**.**

Em 2016, o Mirai *botnet* foi responsável pelos três principais ataques DDoS massivo em servidores DynDNS, surpreendendo as equipes de monitoramento das organizações e indústrias de TI com volumes de tráfegos que excederam 1Tbps [KOLIAS, Constantinos, 2017]. O Mirai *Botnet* procura por alvos que, especificamente, são dispositivos com credenciais padrão do fabricante. O Mirai conecta-se remotamente aos alvos usando os pontos de acesso Telnet e SSH, que geralmente são deixados abertos por padrão. Com um ataque de dicionário básico, ganha controle sobre seus alvos usando as credenciais padrão.

No ano de 2017, durante um período de quatro dias, o *honeypot* da Radware registrou 1.895 tentativas de PDoS (*Permanent Denial of Service*, em português Negação de Serviço Permanente) realizadas pelo *malware* BrickerBot [KOLIAS, Constantinos, 2017]. Este ataque foi direcionado especificamente para dispositivos IoT baseados em Linux pois o *malware* utilizou-se do comando 'busybox'. Os resultados do ataque do *bot* de PDoS foram a interrupção de conectividade com a internet, baixo desempenho do dispositivo e a limpeza de todos os arquivos nos dispositivos.

Diante destes ataques cibernéticos, milhares de empresas, como indústrias, órgãos públicos, hospitais e setores financeiros, tiveram seus dados criptografados ou seus sistemas e redes internas paralisadas, impossibilitando

suas atividades e o atendimento ao público. Muitas instituições financeiras, por exemplo, passaram por perdas significativas pois além dos diversos *reports* e apontamentos do Banco Central do Brasil sobre as consequências de um ataque ocorrido, muitos de seus clientes perdem a confiança na instituição após o vazamento de seus dados ou a falta de atendimento a suas necessidades bancárias.

Por isso, os principais CEOs (*Chief Executive Officer*) e CISOs (*Chief Information Security Officer*) das organizações estão fazendo da segurança cibernética uma parte essencial de suas estratégias de negócios com intuito de buscar ações efetivas para preservar os dados valiosos que circulam pela rede dos computadores de suas organizações.

Diante disso, este trabalho tem como objetivo apresentar, de forma teórica, o resultado de uma análise comparativa entre soluções tecnológicas disponíveis no mercado para segurança das redes internas de ativos IoT desconhecidos ou malicioso, através do gerenciamento de rede e dos acessos aos dados sigilosos. Tendo, como alvo consequente, a mitigação de possíveis ataques cibernéticos.

2. IOT – INTERNET OF THINGS

Internet of Things (IoT), conhecida também como a Internet da Coisas, é um termo que foi criado no ano de 1998 por Kevin Ashton, um britânico que desenvolveu um sistema de sensores onipresentes que permitiu a conexão do mundo físico com a internet [ALSAMANI, Badr e LAHZA, Husam 2018]. De forma resumida, a Internet das Coisas é o conceito de conectar qualquer dispositivo à Internet e a outros dispositivos conectados.

Com os dispositivos IoT em ascensão o modo de vida das pessoas e empresas tende a mudar. Essa inovação oferece diversos benefícios aos seus consumidores como na automatização de tarefas burocráticas e facilidade na tomada de decisões. Porém, com o avanço do IoT os dispositivos pessoais e corporativos se tornam vulneráveis a vários tipos de ameaças de segurança em seu dia a dia, sendo que os problemas antes do advento do IoT, se resumiam

em sua maioria, a ameaças de vazamento de informações e a negação de serviço DDoS *(Distributed Denial of Service)*.

A Internet das Coisas consiste em várias plataformas e dispositivos com diferentes capacidades e propósitos se comunicando, abrindo oportunidades para que dispositivos portáteis, eletrodomésticos e software compartilhem informações entre si através da Internet. Considerando que os dados compartilhados contêm uma grande quantidade de informações privadas, a preservação da segurança das informações desses dados compartilhados é uma questão importante que não pode ser negligenciado. Como o ambiente de comunicação entre os dispositivos é heterogêneo, cada sistema IoT precisará de soluções de segurança diferentes, que irá depender de suas características, tornando-se mais difícil o controle de acesso à rede e verificação da integridade dos dados.

3. CYBERSECURITY E ATAQUES CIBERNÉTICOS

Cybersecurity (em português, segurança cibernética) é a prática de defender computadores, servidores, dispositivos móveis, sistemas eletrônicos, redes e dados contra os ataques mal-intencionados [KASPERSKY, 2016]. Esse tipo de segurança só é necessário por causa dos ataques cibernéticos, oriundos de vulnerabilidades detectadas por *hackers*, que são pessoas com conhecimento avançado em computação e informática [FATHNIA, Froogh 2018]. Estas ameaças são resultados de diversos fatores, por exemplo, *phishing*; *patches* de segurança desatualizados; *backdoor*; utilização de mídias removíveis e *download* de arquivos infectados; desatualização de antivírus; decriptografia dos dados; conexões FTP (*File Transfer Protocol*, em português Protocolo de Transferência de Arquivos) e VPN (*Virtual Private Network*, em português Rede Virtual Privada); arquiteturas pier-2-pier, entre outros [SOLTAN, Saleh 2018].

De acordo com o relatório publicado pelo Dfndr Lab [PSAFE, Tecnologia S.A. Relatório da Segurança Digital no Brasil: Segundo Trimestre – 2018], o número de ciberataques ocorridos no Brasil no primeiro semestre de 2018, foi em torno de mais de 120 milhões, o que representa um aumento de 95,9% se comparado ao mesmo período do ano anterior [PSAFE, 2018]. Alguns dos tipos de ataques

que se concretizaram, consistem na intrusão, infecção e danificação dos dados, *softwares* e *hardwares* da máquina, além dos ataques que causam negação de serviço, conhecidos como DDoS (*Distributed Denial of Service*) e os ataques de fraudes [GUNDUZ, Muhammet Zekeriya 2018].

Nos últimos tempos, as principais violações de *cybersecurity* e as fraudes cibernéticas tiveram um enorme impacto negativo em suas vítimas. A dinâmica das ameaças cibernéticas expõe globalmente muitas organizações empresariais e governamentais aos riscos de segurança da informação diariamente. Como resultado, a maioria das organizações que enfrentam as adversidades de *cybersecurity* e outras ameaças avançadas, sofrem de enorme perda financeira e de reputação. Sabendo que a maioria dos ataques cibernéticos são ações de ataques feitos em várias etapas, compostos por um conjunto de ações de ataque, torna-se necessária uma vigilância do tráfego da rede em tempo real. Com isso os riscos desses ataques diminuem, pois é possível saber o momento e por onde está vindo o ataque, facilitando a neutralização da ameaça da rede.

Grande parte da causa dos problemas relacionados a *cybersecurity* são os erros dos usuários comuns de tecnologia da informação, que devido às poucas habilidades em segurança cibernética, acabam acessando links e executando arquivos maliciosos sem saber do perigo que está por trás, o que representa cerca de 72% a 95% das ameaças de segurança cibernética nas organizações [CONTE, Thomas 2018]. Ao contrário dos profissionais de TI, os usuários finais de computadores são um dos elos mais fracos da cadeia de segurança cibernética, devido as suas habilidades limitadas de segurança cibernética. As habilidades de segurança cibernética são as habilidades que uma pessoa possui para evitar danos à TI através da Internet. No entanto, as atuais medidas de habilidades de segurança cibernética do usuário final são baseadas em pesquisas feitas por eles mesmos. Assim, há uma necessidade urgente de ter uma estrutura de avaliação rápida baseada em critérios de segurança bem estabelecidos que permitam às organizações detectar falhas de segurança tão rapidamente quanto as ameaças que vêm, e retificar essas vulnerabilidades antes que os invasores aproveitem.

4. ESTUDO SOBRE A MITIGAÇÃO DOS RISCOS CIBERNÉTICOS NO SETOR FINANCEIRO

O mundo conectado representa uma grande oportunidade de negócio, principalmente dentro do ambiente corporativo. Sabendo aproveitar bem as informações geradas pelo fenômeno conhecido como IoT, as possibilidades de ganhos são imensas. De acordo com a SAS, [SAS Institute Inc. 2018] 75% dos líderes de negócios globais estão explorando as oportunidades econômicas da Internet das Coisas para criar novos mercados ou aprimorar os serviços já existentes. A GE [GENERAL Electric. 2012] estima que a IoT tenha o potencial de agregar um valor de 10 a 15 trilhões de dólares ao Produto Interno Bruto (PIB) global ao longo dos próximos 20 anos, ultrapassando a economia dos Estados Unidos.

De acordo com a Cisco IBSG [CISCO Internet Business Solutions Group (IBSG). 2018], em 2008 já havia mais dispositivos conectadas à Internet no planeta Terra do que seres humanos vivos. Em 2020, cerca de 50 bilhões de coisas devem estar conectadas por meio de sensores e redes de comunicação. Mesmo uma pequena porcentagem de dispositivos infectados poderia representar uma grande ameaça à segurança cibernética para muitos sistemas e redes corporativas.

O crescente número de “coisas” conectadas à rede de maneira insegura, ou incorreta, representa uma séria ameaça devido as vulnerabilidades que podem ser facilmente exploradas por criminosos cibernéticos, conhecidos como *hackers*, para criar *botnets*, *malwares*, vírus, etc. e usá-los em benefício próprio e/ou para diversas finalidades:

- **Perda de Dados** – Ataques de *Malwares* para excluir, permanentemente, arquivos ou dados confidenciais/internos das máquinas;
- **Roubo de Dados** – Ataques com Vírus para roubar senhas, autenticações bancárias e demais arquivos armazenados que violem a privacidade dos usuários;

- **Indisponibilidade de Dados ou Serviço** – Ataques de *Ransoware* para bloquear o acesso a sistemas ou arquivos e só liberá-los após o pagamento de um valor específico.

O setor financeiro é, particularmente, um dos principais alvos dos criminosos cibernéticos devido à importância e riqueza das informações que ele armazena e, uma vez que o sistema financeiro é altamente interconectado, um ataque bem-sucedido poderia se propagar rapidamente. Além disso, muitas instituições ainda utilizam sistemas antigos, que poderiam não resistir a ciberataques e poderiam ocasionar consequências significativas, na forma de perdas financeiras milionárias, mas também de custos indiretos, como danos à imagem.

E, é por isso que muitos dos principais CEOs e CISOs das organizações estão fazendo da segurança cibernética uma parte essencial de suas estratégias de negócios com o intuito de buscar ações efetivas para preservar os dados valiosos que circulam pela rede dos computadores de suas organizações.

Uma das principais discussões que avança nos setores financeiros refere-se à Resolução 4658, publicada em abril de 2018 pelo Banco Central [BANCO Central do Brasil. 2018], que define a criação de uma política de segurança cibernética para todas as instituições financeiras regulamentadas pelo Banco Central.

Por isso, este trabalho selecionou como cenário os setores financeiros com a finalidade de estudar melhores soluções tecnológicas para prover segurança no gerenciamento dos dispositivos IoT conectados às redes corporativas mitigando as perdas e roubos de dados e a indisponibilidade dos serviços oriundos de ataques cibernéticos bem-sucedidos.

A segurança em redes está relacionada com políticas adotadas pelos administradores de TI para prevenir e monitorar os acessos não autorizados, a modificação ou negação da rede de computadores ou qualquer outra medida de segurança adotada. Ela começa com a autenticação dos usuários ou “coisas” na rede, através de usuário e de senha, para que depois o *firewall* possa aplicar as políticas de acesso, como os serviços que estão autorizados para aqueles usuários, por exemplo.

Uma das tecnologias que geram segurança nos controles de acesso as redes são as soluções NAC – *Network Access Control* (em português, Controle de Acesso à Rede) que permitem as organizações implementarem políticas de segurança para gerenciar o acesso de ativos IoT à infraestrutura, ou seja, patrimônios corporativos ou pessoais autenticados por funcionários e pessoas, fora da organização, autenticadas como convidados externos conectados à rede.

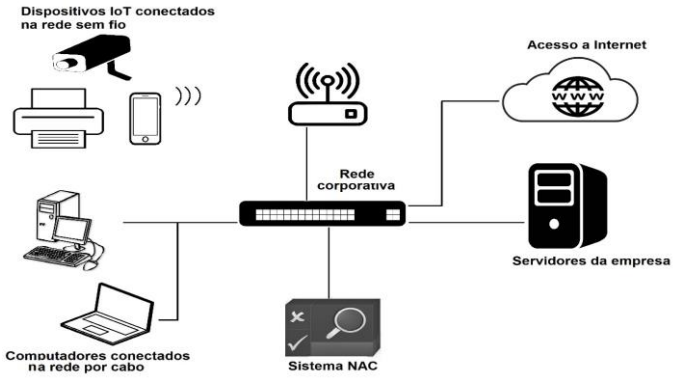

Figura 1: Arquitetura de uma Solução NAC

As soluções NAC desvendam dispositivos IoT examinando a infraestrutura da rede (Figura 1), independentemente, de serem redes WLANs – *Wireless Local Area Network* (em português, Rede Local Sem Fio) ou redes VLANs – *Virtual Local Area Network* (em português, Rede Local Virtual) com o objetivo de, fornecer aos responsáveis pela tecnologia nas empresas a visibilidade dos ativos conectados à rede para que possa ser definido qual a política, ou medida a ser adotada, mais apropriada para cada caso de uso identificado, por exemplo, segregando a infraestrutura entre dispositivos OT (*Operational Technology* – em português, Tecnologia Operacional) e dispositivos IT (*Information Technology* – em português, Tecnologia da Informação).

As soluções NAC, além de auxiliar as organizações a ter visibilidade de sua rede, contribuem para:

- Gerenciamento das políticas de segurança;
- Criação de perfis e visibilidade de ativos;
- Gerenciamento de acesso à rede por convidados;
- Verificação da conformidade de segurança;
- Resposta a incidentes;

- Segurança para dispositivos BYOD (*Bring Your Own Device*).

Por isso, o NAC tem se tornado, cada vez mais, alvo de interesse entre os líderes de Cybersecurity, principalmente, das instituições financeiras devido as demandas regulatórias da nova resolução do Bacen [BANCO Central do Brasil. 2018] e a nova Lei Geral de Proteção de Dados Pessoais [PLANALTO, Governo Brasileiro. 2018].

Diante disso, para selecionar as ferramentas analisadas neste projeto, foram realizadas consultas ao site do Gartner [GARTNER, Inc. 2018] para verificar quais são as ferramentas NAC disponíveis no mercado e quais dessas são as melhores classificadas. As 10 melhores soluções NAC, segundo o Gartner, estão relacionadas na tabela 1:

Nome da Ferramenta	Nome do Fornecedor
BICS (Business Infrastructure Control Solution)	Auconet, Inc.
ISE - Identify Services Engine	Cisco Systems
ExtremeControl	Extreme Networks
Forescout CounterACT®	Forescout Technologies Inc.
FortiNAC	Fortinet, Inc.
Genian NAC	Genians, Inc.
Aruba ClearPass	Hewlett Packard Enterprise
SafeConnect	Impulse, Inc.
CGX	InfoExpress, Inc.
OpenNAC	Open Cloud Factory, Inc.

Tabela 1: *Ferramentas de soluções NAC, melhor categorizadas pelo Gartner, Inc. em 2018.*

Para auxiliar na seleção de ferramentas mais refinadas, foi consultado a sessão de *Reviews* no Gartner [GARTNER, Inc. 2018], para que fosse considerado as opiniões dos usuários e fornecedores, de empresas de mesmo porte aos setores financeiros, que já trabalharam com estas soluções. Com base na maior quantidade de avaliações, na maior nota geral e, considerando os períodos de janeiro até agosto de 2018, pode-se obter os resultados apresentados a seguir (veja a tabela 2):

Nome da Ferramenta	Quantidade de Avaliações	Nota Geral
ISE – Cisco Systems	107	4,2
Forescout CounterACT®	89	4,4
Aruba ClearPass	50	4,3
OpenNAC	35	4
FortiNAC	26	4,2
ExtremeControl	23	4,4
BICS - Auconet, Inc.	16	4

Genian NAC	13	4
SafeConnect	2	3,4
CGX	1	3

Tabela 2: Ferramentas selecionadas com suas respectivas notas e quantidade de avaliações.

Diante desta primeira análise, as 3 soluções selecionadas para este trabalho foram: ISE – Identify Services Engine, Forescout CounterACT® e Aruba ClearPass, devido a maior quantidade de avaliações realizadas e as melhores notas atribuídas.

4.1. ISE – Identify Services Engine

A ferramenta da Cisco Systems – Identity Services Engine (ISE) oferece proteção inteligente e integrada por meio de soluções de políticas e conformidade baseadas em intenção. E tudo isso é entregue com um gerenciamento simplificado e centralizado [CISCO, Systems, 2019].

O Cisco ISE fornece um controle de acesso à rede altamente seguro para usuários e dispositivos. Ele subsidia a obter visibilidade do que está acontecendo na rede, por exemplo, a qual usuário um ativo está conectado; quais aplicativos estão instalados na rede e em execução em determinado momento, etc. Além disso, o ISE faz parte da solução de acesso definido por software (SDA - Software Design Ahnert), através da integração com o Cisco DNA Center, para a aplicação de políticas automatizadas e unificadas.

O Cisco DNA Center é o controlador fundamental e a plataforma analítica no centro da rede baseada na intenção da Cisco [CISCO, Systems, 2019]. Ele simplifica o gerenciamento de rede e permite configurar rapidamente vários serviços ISE, como *Guest* e BYOD, de maneira rápida e fácil em toda a rede.

Outras funcionalidades disponibilizadas pela Cisco ISE são:

- **NAC para Convidados/Terceiros** – Garante que usuários tenham privilégios a rede apartados dos funcionários;
- **NAC para BYOD** – Garante a conformidade de todos os dispositivos de propriedade dos funcionários antes de se conectarem à rede;

- **NAC para Resposta a Incidentes** – Respondem aos alertas de segurança cibernética aplicando automaticamente as políticas de segurança que isolam *endpoint* comprometidos.

4.2. Forescout CounterACT®

A ForeScout CounterACT® da empresa Forescout Technologies, Inc. é uma solução sem agente instalado para uma infraestrutura de rede heterogênea para casos de uso de visibilidade e controle de acesso a dados confidenciais (como, por exemplo, visibilidade do dispositivo; gerenciamento de ativos; conformidade do dispositivo; segmentação de rede e resposta a incidentes) com base em perfis de dispositivos e de usuários sem exigir atualizações de rede ou bloqueio de fornecedores [FORESCOUT, Technologies Inc. 2018]. Além de impor políticas a *switches* com ou sem fio, *firewalls* ou *firewalls* virtuais – com ou sem autenticação pelo protocolo 802.1x – "é um padrão de IEEE para controle de acesso de redes baseado em portas (PNAC) ".

A ForeScout CounterACT® permite automatizar e reforçar o controle de acesso à rede baseado em políticas, conformidade com *endpoint* e segurança de dispositivos móveis. A grande maioria dos dispositivos IoT e dos dispositivos OT conectados à rede não incluem – ou não podem manipular – agentes de software. É por isso que esta plataforma oferece tecnologias de descoberta sem agente e técnicas de monitoramento passivo – [serviço que monitora/rastreia o tráfego, em tempo real, de comunicações sendo transmitido em uma rede - usando recursos de captura de dados em switches - podendo identificar sistemas operacionais, aplicativos e portas ativas em toda a rede] – para evitar a interrupção dos negócios.

Segundo a ForeScout [FORESCOUT, Technologies Inc. 2018] três características tornam a ferramenta CounterACT® diferente das outras soluções NAC:

- **Sem agente** – nenhum agente é necessário para ver ou controlar seus dispositivos IoT, sistemas operacionais, sistemas OT e instâncias;

- **Contínuo** – a plataforma monitora continuamente o comportamento do dispositivo, o status de conformidade e como os dispositivos trafegam pela rede;
- **Heterogêneo** – nenhuma atualização é forçada na rede. Nenhum bloqueio de fornecedor é realizado. Utiliza a infraestrutura de rede existente e soluções de segurança de terceiros com ou sem autenticação do protocolo 802.1X.

4.3. Aruba ClearPass

O Aruba ClearPass da empresa Hewlett Packard Enterprise (HPE) oferece a ferramenta através do gerenciamento em 3 módulos:

- O gerenciamento de Acesso de Terceiros (ClearPass Guest);
- Integração de Dispositivos (ClearPass onBoard) e,
- Avaliação de postura de Ponto de Extremidade (ClearPass onGuard).

O ClearPass Guest torna fácil e eficiente para os funcionários recepcionistas, coordenadores de eventos e outras equipes que não são de TI criar contas de acesso temporário à rede para qualquer número de convidados por dia. O cache MAC também garante que os convidados consigam facilmente se conectar, ao longo do dia, sem a necessidade de inserir as credenciais de acesso no portal de visitantes, podendo ser armazenadas no ClearPass por tempo e quantidade de acesso por tempo indeterminado ou configuradas para que expirem automaticamente em determinado período.

Com o ClearPass Onboard, a equipe de TI define quem pode acessar os dispositivos da instituição, o tipo de dispositivos que podem ser incorporados/conectados à rede, quantos dispositivos por pessoa podem estar conectados ao mesmo tempo e separadamente. Uma autoridade de certificação integrada permite que o departamento de TI ofereça suporte a dispositivos pessoais (BYOD) mais rapidamente através de serviços PKI e recursos de TI subsequentes não são necessários.

Já o ClearPass OnGuard apresenta recursos integrados, para escanear, com a rede que executam verificações da “saúde” da rede baseadas nas conformidades com as políticas de segurança, a fim de eliminar vulnerabilidades através de uma ampla gama de sistemas operacionais e softwares. O ClearPass pode identificar os terminais compatíveis as infraestruturas sem fios, com fios e VPN.

O elemento final de uma infraestrutura segura é a Resposta a Incidentes. A Aruba 360 Security Exchange [ARUBA, Hewlett Packard Enterprise Company. 2018], permite automatizar as ameaças à segurança, remediar ou melhorar um serviço usando soluções/serviços de terceiros, como firewalls, MDM / EMM, MFA, registro de visitantes e ferramentas SIEM. Aproveitando a inteligência de contexto incluída no ClearPass permite que as organizações garantam que a segurança e a visibilidade em um dispositivo com acesso à rede, tráfego e inspeção sejam fornecidas em nível de proteção contra as ameaças cibernéticas.

4.4. Comparativo entre as Soluções

Após realizar um estudo teórico mais aprofundado, melhor detalhado com alguns requisitos técnicos e de negócio – esclarecidos abaixo – e, na apresentação de demos disponibilizadas pelos próprios fornecedores das soluções, foi possível obter um resultado comparativo, conforme apresentado nas tabelas 3 e 5:

- **Fornecedor** – Refere-se a cada solução selecionada para o estudo.
- **Cenários** – Apresenta os segmentos comerciais que mais possuem adesão da solução.
- **Métricas** – Apresenta a quantidade média de autenticações por dia. **Inteligência** – Apresenta quais as inteligências contidas em cada solução.
- Implantação – Apresenta a forma de implantação, se de forma virtual (por *software*, *cloud*, etc.) ou se de forma física (*switch*, etc.).
- **Preços** – Apresenta a forma como cada solução é vendida e seu respectivo valor.

Fornecedor	Cenários	Métricas	Inteligência	Implantação	Preços

Cisco ISE	_Indústrias _Governo _Órgãos Regulatórios	500.000 autenticações por dia e 1,5 milhões de terminais por implantação	_Inteligência Adaptativa _Machine Learning _Detecção Automatizada _Dispositivos IoT	Dispositivos Virtuais	Com base na quantidade de licenças compradas. Valor por licença, aprox. R$ 5.250,00
Forescout CounterACT	_Governo _Setores Financeiros _Rede de Saúde _Varejo	Mais de um 1 milhão autenticações por dia	_Segmentação de Redes _Detecção Automatizada _Dispositivos IoT	Dispositivos Virtuais e Físicos	Dispositivos Virtuais, média de R$ 14.026,79 e Dispositivos Físicos, média de R$ 8.931,05
Aruba ClearPass	_Educação _Finanças _Rede de Saúde _Varejo	Mais de 10 milhões de autenticações por dia	_Detecção Automatizada _Impressões Digitais _Dispositivos IoT	Dispositivos Virtuais e Físicos	Com base na quantidade de *endpoints* + 25 licenças. 100 *endpoints* - R$ 2.700,00 500 *endpoints* - R$ 9.000,00 1.000 *endpoints* - R$ 14.400,00

Tabela 3: Comparativo com base em requisitos de negócio.

Do ponto de vista técnico, foram selecionados alguns requisitos macros para análise, sendo eles: Escalabilidade, Customização, Usabilidade, Flexibilidade de Preço, Integração, Implantação e Suporte [SERRAO, Gloria J, 2018].

- **Escalabilidade** – É uma característica que indica a capacidade de manipular uma porção crescente de trabalho de forma uniforme. A característica que indica se o sistema é um “sistema escalável”, ou seja, um sistema cujo desempenho aumenta com o acréscimo de *hardware*, proporcionalmente à capacidade acrescida.
- **Customização** – É uma característica necessária quando, um sistema “padrão” de um determinado fornecedor, necessita de personalizações específicas apontadas pelos seus consumidores, que podem poderão servir apenas para um único cliente ou incorporados para os demais.
- **Usabilidade** – É a característica que mede a eficácia, eficiência e satisfação dos consumidores para alcançar objetivos específicos em determinado contexto**.**
- **Flexibilidade de Preço** – É a característica que mede a facilidade para negociação de valores perante a compra de serviços oferecidos adquiridos aos clientes e eventuais necessidades futuras.

- **Integração** – É o requisito que se refere a capacidade de comunicação entre a solução com outras ferramentas utilizadas pelo cliente e a forma como essa comunicação será estabelecida.
- **Implantação** – É o requisito que se refere a fase de vida de um software (programa computacional, documentação e dados) e as atividades de implantação (liberação, instalação, ativação, desativação e adaptação) que podem ocorrer no ambiente produtivo e no ambiente de desenvolvimento.
- **Suporte** – É o requisito que se refere ao serviço de assistência intelectual (conhecimentos), tecnológicas (manutenção) e material (peças de reposição) a um cliente ou grupo de clientes com o propósito de solucionar problemas técnicos.

Para cada requisito macro, foram atribuídas algumas funcionalidades específicas para auxiliar na tomada de decisão. O objetivo foi verificar se as soluções selecionadas para análise "Atendem", "Atendem Parcialmente" ou "Não Atendem" a cada funcionalidade mapeada na tabela 4 abaixo.

Funcionalidades
Escalabilidade
Autenticação de fluxos multimídia escalonáveis
Gestão de Workflow e Incidentes
Processo de Escalonamento de Diversos Níveis
Customização
Customização de dashboards e relatórios executivos
Mecanismo para Geração e Exportação/Conectividade de Relatórios
Desenvolvimento de Use Cases, além dos disponíveis por padrão, sem contratação de terceiros
Usabilidade
Segregação dos acessos e alterações por tipo de Usuário
Logs de Acesso e quaisquer ações adicionais no Software
Diferenciação de Interfaces (Técnicas Avançadas e Usuários Finais)
Flexibilidade de Preço
Precificação das Licenças na moeda nativa (Real)
Racional do Licenciamento por Parque de Máquinas
Treinamentos, Suporte e Manutenção e Documentação Incluídos no Valor para o 1º ano
Renovação do Licenciamento garantido ao 2º ano ou com até 10% do Valor Total
Integração
Integração com Sistemas de Mercado (Ex: SIEM's, Antivírus McAfee, DLP, etc.) de outros *Vendors*.
Conexões Com Agente e Sem Agente
Integração com soluções de gerenciamento de identidade e diretório (por exemplo, AD etc.)
Implantação
Apresentação de um PDP (Plano de Projeto) com Cronogramas e *Headcounts* disponíveis
Apresentação de um Plano de Testes, em Alto e Baixo Nível, junto com seus respectivos resultados
Não deverá exigir mudanças nas arquiteturas internas

Serviço de Suporte
Suporte Técnico próprio e Localizado no Brasil
Possuir SLA para Resolução dos Problemas
Suporte Técnico (*In Loco* ou *On-Line*) 24x7

Tabela 4: Framework com as funcionalidades especificas para cada Requisito Macro.

Após a análise das informações obtidas e do preenchimento da tabela de funcionalidades, foi possível identificar qual a melhor solução, através de duas formas: um Mapa de Radar (Figura 2) e uma tabela comparativa de notas (Tabela 5), ambos resultantes do preenchimento dos critérios apresentados na tabela 4.

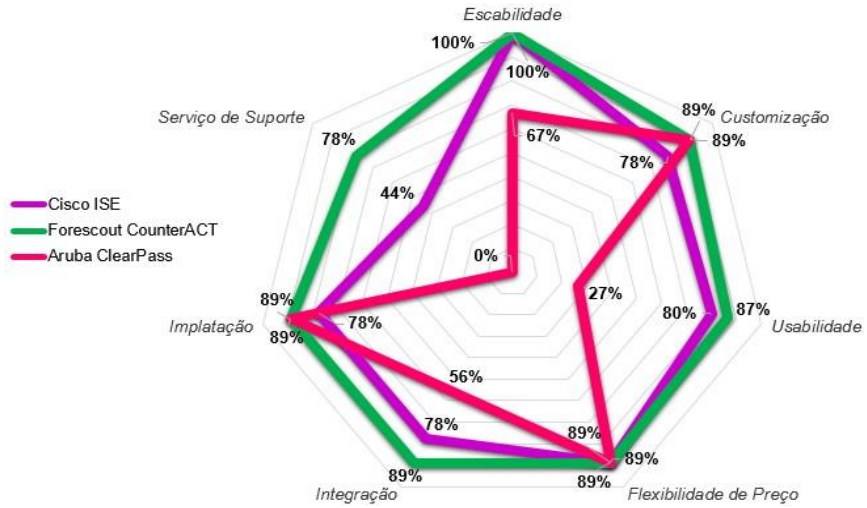

Figura 2: Mapa de Radar resultante da análise das funcionalidades de cada Requisito Macro.

Requisitos Macros	Cisco ISE	Forescout CounterACT®	Aruba ClearPass
Escalabilidade	4,6	4,6	4,2
Customização	4,6	4,4	4,2
Usabilidade	3,8	4,6	4,0
Flexibilidade de Preço	3,8	4,0	4,0
Integração	3,8	4,6	4,0
Implantação	3,4	4,2	3,6
Serviço de Suporte	4,4	4,4	4,0
Nota Geral	**4**	**4,4**	**4**

Tabela 5: Comparativo e atribuição de notas com base nos requisitos macros técnicos.

Com base nas informações coletadas e apresentadas anteriormente e principalmente na apresentação das demos disponibilizadas pelos fornecedores, pode-se concluir que a melhor proposta de solução NAC para segurança de redes e controle de acesso é a Forescout CounterACT®. Pois, das soluções analisadas, é a ferramenta mais adaptável ao cenário de Setores Financeiros, ao volume expressivo de autenticações por dia na rede, é uma solução que oferece seu serviço sem a necessidade da utilização de *agentless*, ou seja,

endpoints configurados nos *switches* para comunicação entre a rede corporativa e a ferramenta. Além disso, é a solução que permite atender um número maior de funcionalidades que as demais estudadas, conforme apresentado na figura 2 e na tabela 5.

Para que a solução possa orquestrar sem o agente, em sistemas operacionais Windows por exemplo, ela utiliza-se da API de conexão WMI (*Windows Management Instrumentation*). Já em outros sistemas operacionais, como Linux e iOS, a ferramenta ainda não possui uma API, sendo recomendável a utilização de agentes para estes SOs.

Uma vez que a Forescout CounterACT® esteja implantada corretamente, e as políticas de acesso criadas e configuradas conforme as necessidades de negócio da empresa, as próximas ações realizadas pela ferramenta são praticamente automáticas. Quando um novo dispositivo tentar se conectar à rede, ela automaticamente pode categorizá-lo em alguma das classes de acesso estabelecidas, como por exemplo: notebooks corporativos com MAC Vendors X, câmeras de segurança da rede de IPs Y, impressoras Samsung do tipo Z, etc.

Caso os dispositivos detectados não estejam em conformidade com as regras estabelecidas, a Forescout CounterACT® poderá se comportar de diversas maneiras, de acordo com as políticas de controle que foram configuradas pela organização. Por exemplo:

1. **Classificar** como um dispositivo reconhecido e, em conformidade com a políticas de controle;
2. **Interromper** a conexão**,** ou a tentativa de conexão, do dispositivo com a rede;
3. **Isolar** o dispositivo em uma zona de quarentena em um VLAN apartada até que as devidas providencias sejam realizadas pelo time responsável;
4. **Colocar** o dispositivo “em espera” para **escaneá-lo** novamente e verificar a possibilidade de classificá-lo em alguma política estabelecida.

A rapidez para tomada de ações, tanto para novos dispositivos que tentam ou se conectam à rede quanto para dispositivos já conectados, permite maior

segurança para as redes internas e para os dados sigilosos das empresas pois, uma vez que os ataques cibernéticos são oriundos de vulnerabilidades de dispositivos maliciosos internos e se estes não estiverem mais conectados pois a Forescout CounterACT® os remediará na primeira camada de acesso, será possível recomendar aos setores financeiros uma solução tecnológica para garantir maior segurança cibernética em suas organizações.

5. CONCLUSÃO

Pode-se observar que o crescimento da utilização da Internet, a quantidade exponencial de dispositivos IoT aumentou simultaneamente. Embora os estes dispositivos proporcionem benefícios aos seus consumidores, ainda existem lacunas, no quesito de segurança cibernética, a serem implementados com o objetivo de proteger seus negócios e seus clientes.

O objetivo deste trabalho pode ser alcançado pois, a implementação de um sistema NAC, como o ForeScout CounterACT® que auxilia no gerenciamento de IoT's da rede, evitando que dispositivos desconhecidos e não autorizados se conectem à rede. Também é possível garantir maior segurança cibernética devido ao seu monitoramento em *real time*. Com isso, qualquer ativo desconhecido, ou vulnerável, que tentar se conectar à rede será bloqueado automaticamente, impedindo que o "acesso malicioso" chegue até a rede e aos dados sigilosos.

Além disso, a ForeScout CounterACT® é a solução que possui maior adesão no mercado financeiro, está disponível tanto em dispositivos físicos como em virtuais, permite seu funcionamento sem agente e atende, em disparado, a uma quantidade maior de funcionalidades selecionadas, como por exemplo: Escalabilidade, usabilidade, integração e serviços de suporte.

No entanto, cabe certificar-se de ter uma documentação da rede interna detalhada, incluindo um mapa de rede atualizado antes de implementar a solução e certificar-se de ter um inventário dos sistemas categorizados de maneira lógica. Além disso, realizar os backups do banco de dados NAC e testá-los regularmente antes de realizar qualquer upgrade da ferramenta.

Além do estudo apresentado, sugere-se como trabalhos futuros a análise do fenômeno *Shadow It* (em português, TI Invisível) nas empresas, com a finalidade de entender como ele tem sido inserido cada vez mais em instituições e quais as preocupações e medidas de segurança cibernéticas devem ser aplicadas.

REFERÊNCIAS BIBLIOGRÁFICAS

ALSAMANI, Badr; LAHZA, Husam. **A taxonomy of IoT: Security and privacy threats**. USA, Information and Computer Technologies (ICICT), 2018 International Conference on, 2018.

ARUBA, Hewlett Packard Enterprise Company. **Aruba ClearPass Network Access Control**, 2018. Disponível em: <https://www.arubanetworks.com/assets/so/SO_ClearPass.pdf.> Acesso em: 20 de março de 2019.

BANCO Central do Brasil. **RESOLUÇÃO Nº 4.658**, 2018. Disponível em: <https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf.> Acesso em: 20 de março de 2019.

CISCO, Systems. **Cisco Identity Services Engine Data Sheet**, 2019. Disponível em: <https://www.cisco.com/c/en/us/products/collateral/security/identity-servicesengine/data_sheet_c78-656174.html.> Acesso em: 20 de março de 2019.

CONTE, Thomas M. et al. **Rebooting Computers to Avoid Meltdown and Spectre**. IEEE Computer Society, 2018.

FATHNIA, Froogh et al. **The effect of cyber-attacks on the demand dispatch application and identify them by OPTICS.** Iran, Knowledge-Based Engineering and Innovation (KBEI), 2017 IEEE 4th International Conference on, 2018.

FORESCOUT, Technologies Inc. **Visibility to put you in in control of network access control**. Disponível em:

<https://www.forescout.com/solutions/networkaccess-control/. 2018> Acesso em: 19 de março de 2019.

GARTNER, Inc. **Market Guide for Network Access Control**, 2018. Disponível em: <https://www.gartner.com/doc/3884483?ref=mrktg-srch> Acesso em: 16 de março de 2019.

GENERAL Electric. **Industrial Internet: That Combination of Networks and Machines Could Add $10 to $15 Trillion to Global GDP**, 2012. Disponível em: <https://www.ge.com/reports/post/76430585563/new-industrial-internet-reportfrom-ge-finds/> Acesso em: 21 de março de 2019.

GUNDUZ, Muhammet Zekeriya et al. **A comparison of cyber-security oriented testbeds for IoT-based smart grids.** Turkey, Digital Forensic and Security (ISDFS), 2018 6th International Symposium on, 2018.

KOLIAS, Constantinos et al. **DDoS in the IoT: Mirai and Other Botnets**. IEEE Computer Society, IEEE, 2017.

PLANALTO, Governo Brasileiro. **LEI Nº 13.709**, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm> Acesso em: 22 de março de 2019.

PSAFE, Tecnologia S.A. **Relatório da Segurança Digital no Brasil: Segundo Trimestre – 2018**. 2018. Disponível em: <https://www.psafe.com/dfndr-lab/wpcontent/uploads/2018/08/dfndr-lab-Relat%C3%B3rio-da-Seguran%C3%A7aDigital-no-Brasil-2%C2%BA-trimestre-de-2018.pdf> Acesso em: 08 de dezembro de 2018.

SAS Institute Inc. **Infographics – Analytics of Things**, 2018. Disponível em: <https://www.sas.com/content/dam/SAS/it_it/doc/infographics/Analytics-ofThings-english.pdf> Acesso em: 18 de fevereiro de 2019.

SERRAO, Gloria J. **Network access control (NAC): An open source analysis of architectures and requirements**. San Jose, CA, USA. 44th Annual 2010 IEEE International Carnahan Conference on Security Technology, IEEE, 2018.