Cloud Target

Produtividade | Segurança | Governança

CDC & MSS

#ZeroTrust #AI

SERVIÇOS GERENCIADOS MODERNOS PARA O NOVO MUNDO

CONECTIVIDADE

Baixa Latência
Redução de Custos

GOVERNANÇA

Gerenciamento de Políticas
Gerenciamento de Custos
Analise de Comportamentos
Regulamentações (BACEN, LGPD etc).

MONITORAÇÃO

Infra, Rede, Sistemas e
Experiência do Usuário

SEGURANÇA

Gerenciamento de Identidade
Proteção da Informação
Proteção de Ameaças
Teste de Penetração
SIEM & SOAR

GERENCIAMENTO

Serviços de Sustentação
Gerenciamento de SO, Backup etc
Serviços Especializados
Banco de Dados, SAP

PROTEÇÃO

Recuperação de Desastres
Continuidade de Negócios

SERVIÇOS GERENCIADOS – CDC / MSS

Cloud Target

Gerenciamento de Identidade e acesso

Gerenciamento de equipamentos, dispositivos móveis e aplicativos

Gerenciamento de Proteção da Informação

Gerenciamento de Proteção Contra Ameaças

Gerenciamento de FW

PEN Teste

Gerenciamento de Wi-Fi

Gerenciamento de Antivírus e Antimalware

Gerenciamento de Gateway de Aplicação

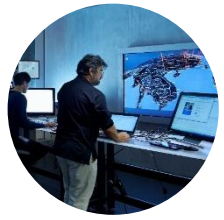
Gerenciamento de Segurança e Conformidade

Gerenciamento de Aplicações

Gerenciamento de Logs Centralizado com IA (SIEM e SOAR)

Protega a porta de entrada

Proteja seus dados em qualquer lugar



Detecte e remedie ataques

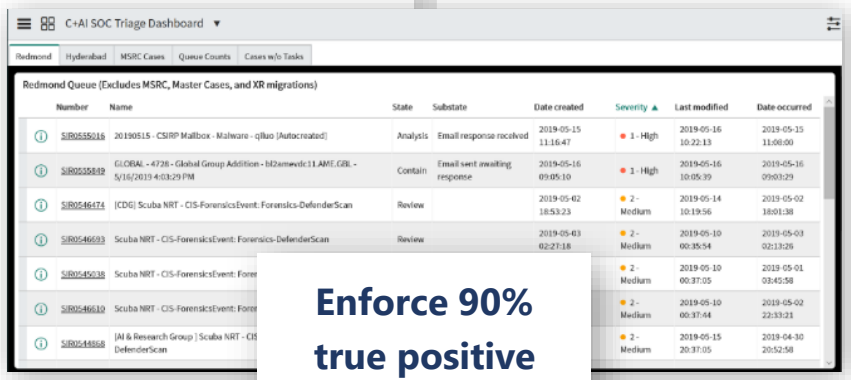
ABORDAGEM DO CYBER DEFENSE CENTER

Cloud Target

Impor qualidade + aplicar tecnologia + amplificar as habilidades dos analistas

Detectar

Bilhões de eventos por mês



Enforce 90% true positive on alert feeds

Machine Learning (Artificial Intelligence)

Análise comportamental (UEBA) (Usuário e Entidade)

Responder

Concentre-se no tempo para reconhecer e remediar

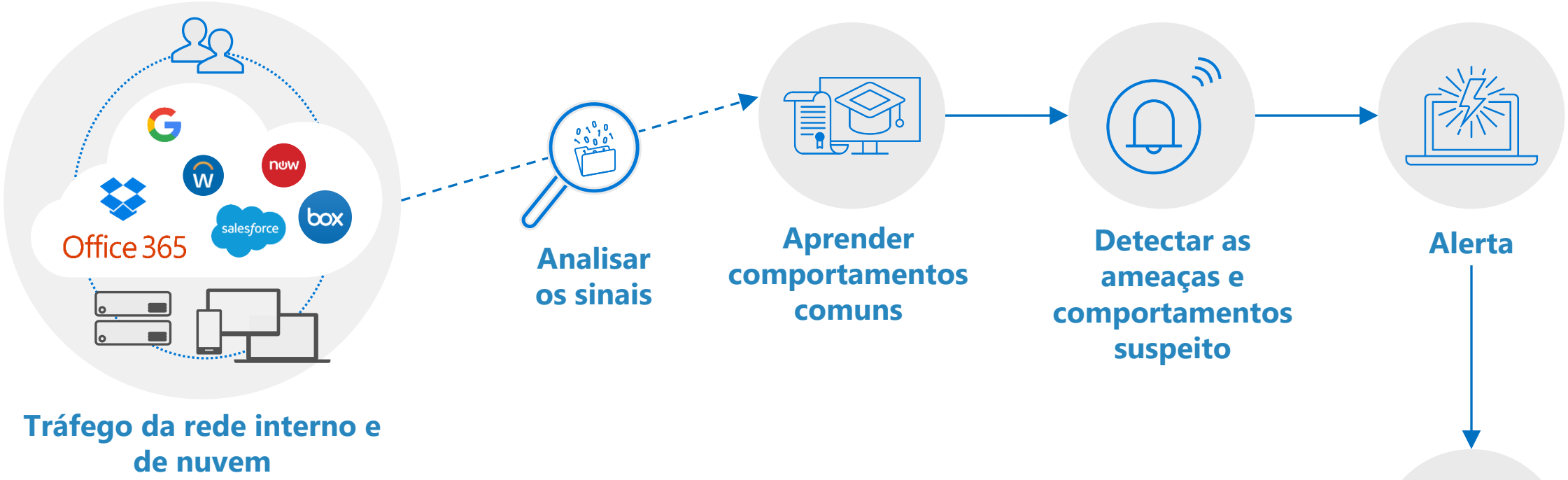
Orquestração de Segurança, Automação e Remediação (SOAR)

Bilhões de eventos por mês

Dezenas de investigações

ANÁLISE 24 X 7 PARA PROTEGER CONTRA AMEAÇAS COM IA

Cloud Target



Diário de Bordo e Relatórios Mensais

- Monitoramento (ataques bloqueados e comportamentos fora do padrão)
- Recomendações / Melhorias Contínuas

CYBER DEFENSE CENTER HIBRIDO

Cloud Target

Visão ampla da empresa
Correlacionado/Unificado
Visão de incidente

Gerenciamento de Casos

Azure Sentinel
- Machine Learning (ML) & AI
- Análise comportamental (UEBA)
- Orquestração de Segurança, Automação, e Remediação (SOAR)
- Lago de Dados de Segurança
- Gerenciamento de Incidentes e Eventos de Segurança (SIEM)

Clássico SIEM
ArcSight · Radar · splunk> · ...

Alerta de integração - API de segurança de gráfico

Gráfico de segurança inteligente (ISG)
Inteligência Integrada de Ameaças & Deep Human Expertise

Melhorar e Aprender medindo:
Responsividade - Tempo médio para reconhecer (MTTA)
Efetividade... Tempo Médio para Remediar (MTTR)

Especialista em CDC
Cloud Target

O SOAR reduz o esforço/tempo dos analistas por incidente, aumentando a capacidade geral do SOC

Assistência Especializada
Habilitando analistas com habilidades escassas

- **Resposta a incidentes, recuperação, & CyberOps Serviços**
- **Especialistas em Ameaças da Microsoft**
- **Detecção e resposta gerenciadas** Usando proteções contra ameaças da Microsoft
  Cloud Target

Insights Profundos
Alertas acionáveis derivados do profundo conhecimento dos ativos e ML/UEBA

Troncos brutos
Segurança e Registros de atividades

Segurança & Rede
Fornecer segurança acionável alertas, registros brutos, ou ambos

Carbon Black. · Symantec · FORTINET · SOPHOS · zscaler · FIREEYE · CYBERARK · Lookout · DUO · paloalto · Check Point · F5 · CROWDSTRIKE · Barracuda · ...

Proteção contra ameaças da Microsoft (MTP) (SOAR)

- **Azure Centro de Segurança**
- **Azure ATP**
- **Azure AD Proteção de identidade**
- **Microsoft Defender** Proteção avançada contra ameaças (ATP)
- **Office 365 ATP**
- **Nuvem Segurança do aplicativo**
- **Proteção de informações**

Infraestrutura híbrida e aplicativos
Java · JBoss · HTML · Microsoft .net · php · .NET · ... · vmware · aws · ...

Gestão de Identidade & Acesso
{LDAP} · Ping · ... · okta · ORACLE · SailPoint

Extremidade & Mobile
...

Aplicações Modernas & SaaS
Escritório 365 · ... · OpenID · new · SAML · ...

Informações
ORACLE · SQL Server · MySQL · IBM DB2 · ...

Legenda
- Terceirização
- Consultoria e Escalonamento
- Monitoramento baseado em registro de eventos
- Investigação & Caça Proativa
- Monitoramento de recursos nativos

PRIMEIRO FAREMOS UMA AVALIAÇÃO DE SEGURANÇA

Cloud Target

Foco
em aprender sobre suas prioridades, iniciativas e influências fundamentais em sua estratégia de segurança.

Descobrir
ameaças ao seu ambiente através de e-mail, identidade e dados.

Verificar
possíveis melhorias baseado na experiência de nossos Especialistas e boas práticas de mercado

Plano
próximos passos sobre como podemos trabalhar juntos.

SIMPLIFIQUE A SEGURANÇA, MELHORE A PROTEÇÃO CONTRA AMEAÇAS

Cloud Target

CASB (Microsoft Cloud App Security, Segurança de Aplicativos em Nuvem)

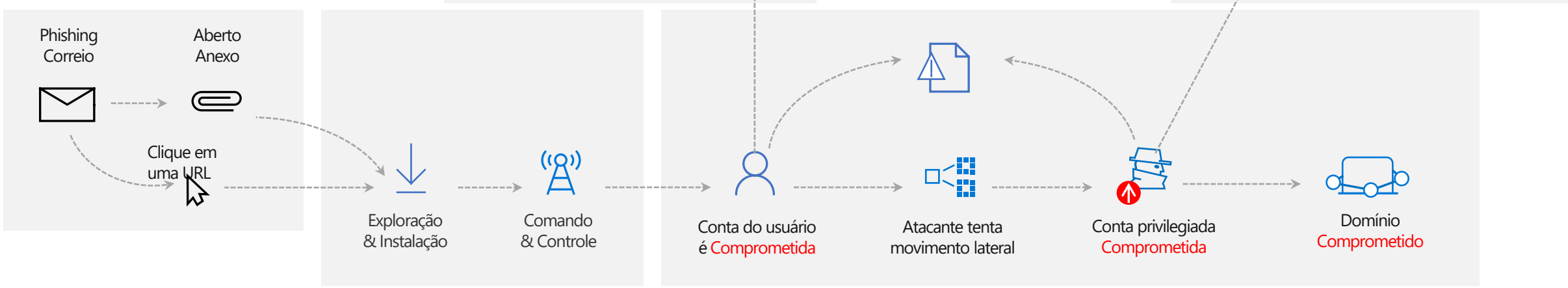
Amplia proteção e acesso condicional a outros aplicativos em nuvem

Proteção de Identidade (AD Premium P2)

Proteção de identidade e acesso condicional

Microsoft Defender for O365

Detecção de malware, links seguros e anexos seguros



Microsoft Defender for Endpoint (EDR)

Detecção e resposta ao endpoint(EDR) & Proteção de endpoint (EPP)

Microsoft Defender for Identity

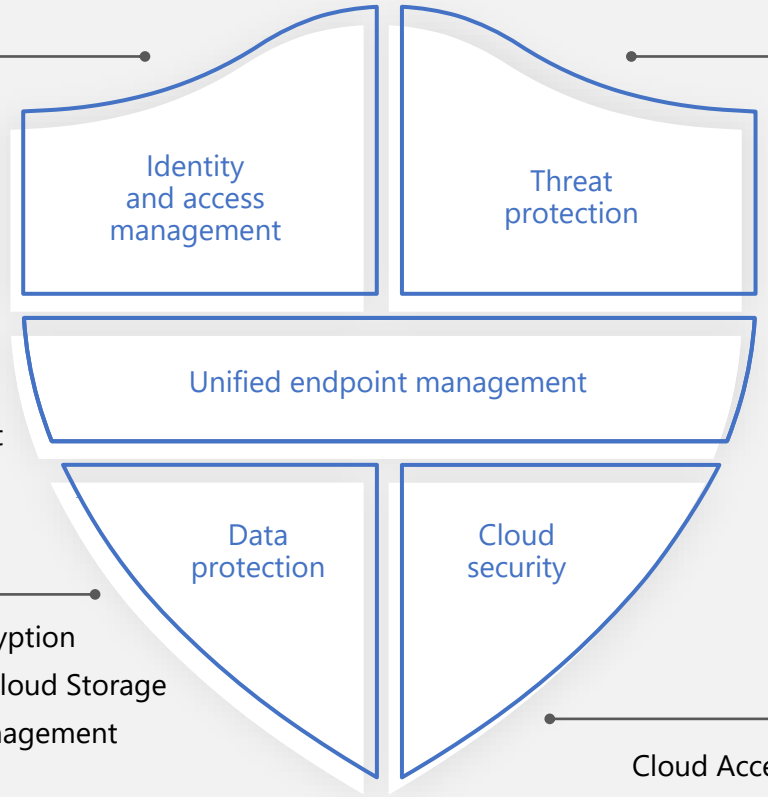
Proteção de identidade

AGILIZAR E FORTALECER

Cloud Target

CONSOLIDAR A SEGURANÇA

SUBSTITUA ATÉ 40 PRODUTOS DIFERENTES POR UMA SEGURANÇA INTEGRADA E DE PONTA A PONTA



Single Sign on + Self-Service Reset
Multifactor + Passwordless Authentication
Conditional Access
Privileged Access Management
Identity Governance
Active Directory

Mobile Application Management
Mobile Device Management

Data Discovery
Data Classification
Data Loss Prevention
Insider Risk Management
Database Security
Information and Messaging Encryption

Device Encryption
Encrypted Cloud Storage
Secrets Management

Endpoint Detection and Response
Endpoint Protection Platform Forensic Tools
Intrusion Prevention System
Threat Vulnerability Management Anti-phishing
User and Entity Behavior Analytics
Threat Intelligence Feeds
App and Browser Isolation
Attachment Sandboxing

Application Control
End-user Training
Network Firewall (URL Detonation)
Host Firewall
Secure Email Gateway
Security Assessment
SIEM
SOAR
Incident Response Services
DDoS Protection
IoT Protection

Cloud Access Security Broker
Cloud Workload Protection Platform
Cloud Security Posture Management

Microsoft

Diferenciais Cloud Target

- Hybrid Managed Services e CDC
- Equipe Especializada 24x7
- IA – Inteligência Artifical e ML – *Machine Learning*
- Alertas das alterações realizadas
- Diário de Bordo + Book de Métricas Mensal + Recomendações
- Gerente de Nível Serviço 24x7