



Boas Práticas

Relatório Executivo Resumido

N-able N-sight RMM

Aviso legal

As informações e o conteúdo deste documento são fornecidos apenas para fins informativos e são fornecidos "no estado em que se encontram", sem garantia de qualquer tipo, expressa ou implícita, incluindo, mas não se limitando às garantias implícitas de comercialização, adequação a um fim específico, e não violação. A ADDEE não se responsabiliza por quaisquer danos, incluindo danos consequentes, de qualquer tipo que possam resultar do uso deste documento e das ferramentas nele citadas. As informações do presente documento são obtidas de fontes publicamente disponíveis.

Sumário

Introdução	3
Pontuação de Integridade	4
Cabeçalho	4
Breakdown	5
+ Monitoramento Proativo	5
+ Antivírus	5
+ Web Protection (Filtro de rede)	6
+ Disponibilidade do Servidor	6
+ Tickets de Service Desk Fechados	6
+ Gerenciamento de Patches	6
+ Falha em Tentativas de Logon	6
+ Risk Intelligence	7
+ Backup	7
Dispositivos Gerenciados	8
Efetividade de Proteção	10
Cobertura	12
Sistemas Operacionais	12
5 Principais	13
Obrigado!	14

Introdução

O **Relatório Executivo Resumido** tem como objetivo trazer informações sobre a infraestrutura do cliente, onde será possível analisar, de forma resumida, o trabalho realizado durante o mês. Identificando assim o que melhorou, o que ainda precisa ser melhorado ou o quê precisa de atenção.

Além disto, recomendamos que este relatório seja utilizado como uma forma de demonstrar ao cliente final todo o trabalho desempenhado e executado pelo prestador de serviços, agregando valor a sua prestação.

Para o cliente que possui TI interna a leitura a ser realizada é da mesma maneira, mas os dados serão referentes a sua própria infraestrutura.

Neste artigo explicaremos como se deve ler este relatório, a fim de extrair o máximo de informações sobre o ambiente.

Observação: Para os prestadores de serviços, sugerimos que ao invés de somente enviar o relatório mensalmente, que também seja feita a explicação sobre todas as informações para o cliente, semelhante ao exemplo abaixo, para que não haja dúvidas sobre os dados.

Queremos sua opinião! Ajude-nos a aprimorar este documento. Qualquer dúvida, crítica ou sugestão, por favor, encaminhe um e-mail para boaspraticas@addee.com.br.

Cabeçalho

Relatório Executivo Resumido

Gerado para ADDEE IT Pro para Janeiro 2023



Este relatório é mensal, e único para cada cliente. Portanto esta informação sempre será demonstrada no cabeçalho do relatório para identificação.

O relatório também permite inserir a sua logomarca, uma vez que você possua o Branding aplicado ao seu painel, para valorizar ainda mais o trabalho desempenhado.

Pontuação de Integridade

Pontuação de integridade



Breakdown

Monitoramento proativo	100%	Disponibilidade do servidor	99,8%	Falhas em tentativas de logon	0%
Antivírus	100%	Gerenciamento de patch	81,9%	Backup	84,9%
Cobertura	100%	Cobertura	100%		
Proteção	100%	Proteção	63,7%		
Web Protection	98,2%				
Cobertura	96,3%				
Proteção	100%				

A Pontuação de Integridade traz uma média (em porcentagem) sobre os recursos monitorados ativos no ambiente (Breakdown).

Se um recurso não está habilitado, a pontuação da integridade não será afetada negativamente.

Breakdown

Pontuação de integridade



Breakdown					
Monitoramento proativo	100%	Disponibilidade do servidor	99,8%	Falhas em tentativas de login	0%
Antivírus	100%	Gerenciamento de patch	81,9%	Backup	84,9%
Cobertura	100%	Cobertura	100%		
Proteção	100%	Proteção	63,7%		
Web Protection	98,2%				
Cobertura	96,3%				
Proteção	100%				

Em “Breakdown” será mostrado a média dos valores de cobertura e proteção, referente aos recursos abaixo:

+ Monitoramento Proativo

- Porcentagem de dispositivos com verificações 24x7 e DSC. Ou seja, são dispositivos que possuem uma forma de monitoramento, seja com verificações 24x7 ou DSC.
- No exemplo deste artigo vemos que a porcentagem no relatório foi de 100% para o monitoramento proativo. Isto significa que todos os dispositivos que estão sendo gerenciados neste cliente possuem verificações 24x7/DSC.
- Verificações dos recursos, como Backup, Antivírus, etc. não são consideradas com monitoramento proativo.

+ Antivírus

- Média dos valores de Cobertura e Proteção, onde:
 - **Cobertura** – Porcentagem de dispositivos com “Verificação de Atualização do Antivírus” (todos os mecanismos).
 - **Proteção** – Porcentagem de dispositivos com verificações aprovadas de “Verificações de Atualização do Antivírus” (todos os mecanismos) e “Verificações do Antivírus Gerenciado”.
- Antivírus de terceiros, que são monitorados pelo N-sight RMM, também serão contabilizados neste parâmetro.

+ Web Protection (Filtro de rede)

- Média dos valores de Cobertura e Proteção, onde:
 - **Cobertura** – Porcentagem de dispositivos com Web Protection ativo.
 - **Proteção** – Porcentagem de requisições maliciosas bloqueadas e permitidas.

+ Disponibilidade do Servidor

- Informará a porcentagem de tempo que todos os servidores estavam disponíveis.
- No nosso exemplo podemos ver o valor de 99.8%, que pode significar que no mês de Janeiro houve uma queda de energia ou perda de comunicação momentânea com a internet, e por isto o 100% não foi atingido.

+ Tickets de Service Desk Fechados

- Porcentagem de tickets levantados e resolvidos, onde um Service Desk esteja configurado no N-sight RMM (MSP Manager, Max Service Desk, Autotask, ConnectWise, etc.).
- Neste exemplo não aparece esta informação porque não havia nenhuma solução de Service Desk integrada à solução no mês de Janeiro.

+ Gerenciamento de Patches

- Média dos valores de Cobertura e Proteção, onde:
 - **Cobertura** – Porcentagem de dispositivos com Gerenciamento de Patches ativo.
 - **Proteção** – Porcentagem de patches detectados que foram instalados.

+ Falhas em Tentativas de Logon

- Porcentagem do número de verificações “Falha na verificação de logon” aprovadas dividido pelo número total de verificações “Falha na verificação de logon”. Onde 0% indica que não houveram falhas.



+ Risk Intelligence

- Média dos valores de Cobertura e Proteção, onde:
 - **Cobertura** – Porcentagem de dispositivos com Risk Intelligence ativo.
 - **Proteção** – Porcentagem de tarefas do Risk Intelligence automatizadas aprovadas.
- Neste exemplo não aparece esta informação porque não estava ativo o recurso de Risk Intelligence no mês de Janeiro.

+ Backup

- Porcentagem de verificações aprovadas do Backup.
- Backups de terceiros, que são monitorados pelo N-sight RMM, também serão contabilizados neste parâmetro.

Dispositivos Gerenciados

Dispositivos gerenciados



Em “Dispositivos” será apresentado o número total de dispositivos gerenciados, separados por tipo (Servidores, Desktops, Notebooks e Disp. Móveis), independente do Sistema Operacional utilizado.

Em “Verificações Aprovadas” será apresentado o percentual das verificações aprovadas no decorrer do mês, agrupadas por categoria:

- **Aplicação**
 - Verificação de atualização de antivírus (todos os mecanismos)
 - Verificações de Backup (todos os mecanismos)
 - Verificação de repositório do Exchange
 - Verificação de Fila MTA
 - Verificação MySQL
 - Verificação WSUS
- **Disco/Arquivo**
 - Verificação de espaço em disco
 - Verificação de alterações no espaço em disco
 - Verificação de tamanho de arquivo
 - Verificação de estado do disco físico
- **Evento**
 - Verificação log de sistema Apple
 - Verificação de eventos críticos
 - Verificação de log de eventos



- **Script**

- Verificação de script

- **Serviço**

- Verificação de Daemon Linux
- Verificação de Daemon OS X
- Verificação de processo
- Verificação de serviço do Windows

- **Sistema**

- Falha na verificação de logon
- Verificação de atualização OS X
- Verificação de gerenciamento de pacote
- Verificação de memória física
- Verificação de monitoramento de desempenho do servidor

- **Tarefa**

- Tarefas automatizadas

E em **“Alertas Resolvidos”** temos a quantidade de verificações que foram levantadas, fechadas ou limpas durante o mês.

Efetividade da Proteção

Efetividade da proteção

Antivírus		
Dispositivos com antivírus	27	
Frequência de dispositivos atualizados	100.0%	
Ameaças em quarentena/resolvidas	0	
Acesso remoto		
Sessões do Take Control		126
Web Protection		
Dispositivos com Web Protection	26	
Solicitações filtradas bloqueadas	0	
Solicitações mal-intencionadas bloqueadas	0	
Backup		
Dispositivos com backup		23
Dados de backup (GB)		35
Backups bem-sucedidos		230
Gerenciamento de patch		
Dispositivos com gerenciamento de patches	27	
Patches detectados	262	
Patches instalados	167	

Nesta parte do relatório é demonstrado informações detalhadas sobre os recursos ativados ao longo do mês:

- **Antivírus**
 - Quantidade de dispositivos com antivírus
 - Frequência de dispositivos atualizados
 - Ameaças em quarentena/resolvidas – Informação disponível apenas para o MAV (antivírus gerenciado).
- **Backup**
 - Quantidade de dispositivos com backup
 - Dados de backup (GB) – volume de dados “backupeados” somente disponível para o MOB (Max Online Backup).
 - Backups bem-sucedidos
- **Service Desk – Disponível apenas para o Max Service Desk**
 - Tickets gerados por clientes que foram fechados
 - Horas gastas com tickets
 - Tickets de monitoramento fechados



- **Gerenciamento de Patches**

- Dispositivos com gerenciamento de patches
- Patches detectados – não inclui patches com status “ignorado”.
- Patches instalados

- **OBS: o Relatório Executivo Resumido contém o número de patches detectados e instalados de um mês específico, tais informações podem ser diferentes das mostradas no N-sight RMM ou no relatório de visão geral do Gerenciamento de Patches uma vez que ambos mostram informações maiores do que um mês.**

- **Risk Intelligence**

- Dispositivos com Risk Intelligence
- Valor total da responsabilidade

- **Acesso Remoto**

- Sessões do Take Control
- Sessões de Segundo plano remoto

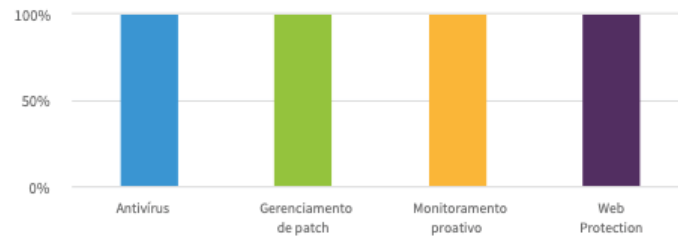
- **Web Protection**

- Dispositivos com Web Protection
- Requisições filtradas e bloqueadas – Com base na opção “Filtro por categoria”.
- Requisições maliciosas bloqueadas

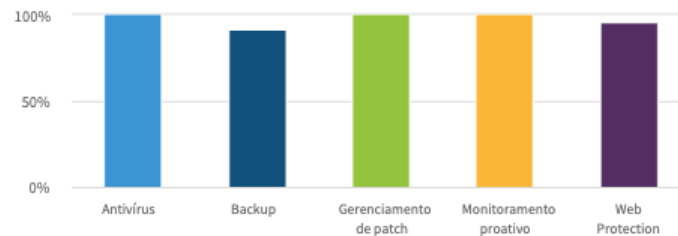
Cobertura

Cobertura

Servidores



Estações de trabalho



Nesta sessão é apresentado os indicadores visuais da porcentagem de Servidores ou Estações de trabalho onde tal recurso está ativo.

Sistemas Operacionais

Sistemas operacionais



Mostra a quantidade de sistemas operacionais utilizados no ambiente. Neste nosso exemplo tínhamos 3 SOs no mês de Janeiro: **Windows 10**, **Windows 11** e **Windows Server 2019**.

5 Principais

5 Principais

Dispositivos com falhas nas verificações	Dispositivos em Risco	Categorias de Website Permitidas
A-SVR-01	A-DES-21	Computer and Internet Info
A-ADL-01	A-DES-17	Business and Economy
A-LAP-05	A-SVR-01	Web based email
A-DES-11	A-DES-15	CDNs
A-DES-21	A-LAP-07	Internet Communications

Nesta última sessão do relatório são descritos os 5 principais dispositivos de cada uma das 3 categorias apontadas, na qual o MSP deve se atentar para corrigir e/ou remediar a situação.

- **Dispositivos com falhas nas verificações**
 - Aqui mostrará os 5 dispositivos que mais apresentam falhas nas verificações de monitoramento.
- **Dispositivos em Risco**
 - Classificação dos dispositivos que tiveram as falhas mais comuns nas verificações de Antivírus, Vulnerabilidade, Risk Intelligence e Web Protection ao longo do mês.
- **Categoria de Websites permitidas**
 - Aqui mostrará as categorias de sites mais acessadas ao longo de todo o mês.



Empresa brasileira, iniciamos nossas operações em 2013 com o objetivo de revolucionar o mercado de Prestação de Serviços de TI e contribuir com o enriquecimento moral, intelectual e financeiro de nossos clientes e colaboradores.

Nascemos da necessidade de um Prestador de Serviços de TI e hoje somos Distribuidores das melhores ferramentas para Prestadores de Serviços de TI de todo o Brasil.

Trabalhamos para o crescimento sustentável do mercado de tecnologia, através do compartilhamento de conhecimentos e a distribuição de soluções inovadoras para Gestão de TI. Com estrutura local, fornecemos atendimento e suporte em português, além de todo o apoio comercial necessário para empresas de Serviços de TI.

Compreendemos as necessidades locais e por isso somos o principal parceiro de negócios dos nossos clientes.

Com um time de profissionais altamente qualificados e apaixonados por tecnologia e relacionamento, colocamos acima de tudo, as pessoas. É assim que fazemos negócios.

Última alteração: Março/2023

Responsável: Caio Gutierri

E-mail: boaspraticas@addee.com.br



YouTube



Instagram



LinkedIn



Site



Blog