

# 5 etapas para manter segura sua empresa no agronegócio

Soluções simples e acessíveis  
para estar protegido frente a  
ciberameças avançadas

SONICWALL®

# Introdução

Responsável quase um quarto do produto interno no Brasil, o agronegócio tem buscado inovações em ritmo nunca visto antes. E a adoção de tecnologias disruptivas vem sendo fator crítico para competitividade também neste setor.

Foi-se o tempo em que o agronegócio caminhava alheio às grandes transformações relacionadas à tecnologia da informação e digitalização.

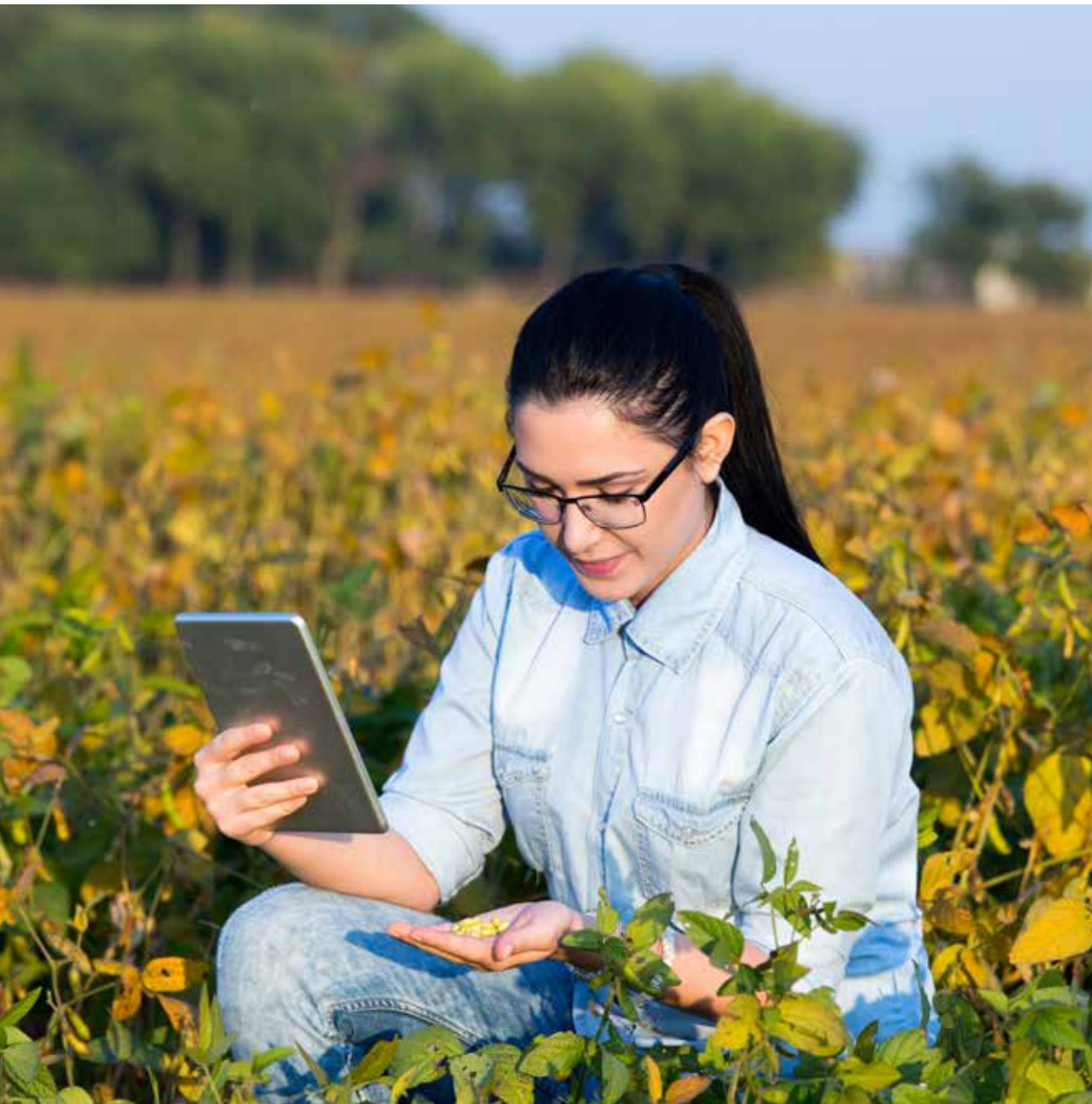
Num mercado globalizado, cresce a cada dia a pressão para que as empresas profissionalizem suas operações e garantam seus diferenciais competitivos. Estamos falando de uma projeção de alimentar uma população mundial de 10 bilhões de pessoas até 2050.

Estes números explicam o esforço massivo para ampliar a produção de alimentos em até 70%. E este fato é, sem dúvida, o principal vetor que impulsiona os investimentos para digitalização do agronegócio.

E sem dúvida, num contexto global de constantes ciberameaças passa ser fundamental um olhar diferente para o tema Segurança da Informação.

Neste e-Book preparado pela SonicWall no Brasil, entenda os vetores de investimento e os consequentes desafios de segurança para empresas do agronegócio e cinco etapas simples para estar protegido.





# Índice

[Vetores de investimento em tecnologia da informação.](#)

[Principais desafios de segurança para empresas no agronegócio.](#)

[5 etapas para manter segura sua empresa no agronegócio.](#)

[Etapa 1: Implemente segurança em camadas.](#)

[Etapa 2: Estenda a segurança para redes móveis.](#)

[Etapa 3: Esteja preparado para o inesperado.](#)

[Etapa 4: Simplifique sua infraestrutura de segurança.](#)

[Etapa 5: Garanta TCO alinhado com à sua capacidade de investimento.](#)

[Conclusão](#)

IoT (Internet of Things) E BIG DATA

## Vetores de investimento

### IoT: uma realidade no campo

Os dispositivos inteligentes já são responsáveis por automatizar em até 90% a indústria do agronegócio em economias do primeiro mundo. O Brasil caminha na mesma direção. É o que comprova o relatório da Secretaria Executiva da Comissão Brasileira de Agricultura de Precisão (CBAP), que aponta que cerca de 67% das propriedades agrícolas do país usam algum tipo de tecnologia, seja na área de gestão dos negócios, seja nas atividades de cultivo e colheita.

O agronegócio no Brasil tem realizado importantes investimentos na robotização e na implementação de dispositivos inteligentes com focos estratégicos de otimização da gestão e aumento de produtividade.

De acordo também com estudo da Inmarsat "Future of IoT in Enterprise - 2017", embora cerca de 54% das empresas no agronegócio em todo mundo já tenham adotado alguma tecnologia IoT ou estejam em processo de implementação, apenas 23% estão confiantes nos níveis de segurança dos seus atuais sistemas.

### Big Data: ativo competitivo

Se por um lado os dispositivos IoT e adoção de robos sejam responsáveis por automatizar processos produtivos no agronegócio. Por outro, estes são hoje fonte geradora de dados com valor inestimável para a operação destas empresas que, somados aos dados coletados em outras tecnologias, como os tags RFID (e tecnologias correlatas), garantem hoje, informações precisas para melhorar a tomada de decisão sobre onde aplicar seus investimentos.

Neste quadro, Big Data e as ferramentas de análise de dados aliam-se a soluções de Inteligência Artificial (AI) para dinamizar o agronegócio. Aonde a busca constante e incansável pela agricultura de precisão passa necessariamente pelo uso intensivo de dados para melhoria de produtividade.

Estes dados são a base para os investimentos em pesquisa e desenvolvimento de propriedade intelectual aplicada ao campo. Sendo um patrimônio digital chave para melhorar a competitividade e a lucratividade.





## DESAFIOS DE SEGURANÇA PARA O AGRONEGÓCIO

# Ciberameaças no compasso da digitalização em massa

Segundo o SonicWall Security Center, plataforma desenvolvida pela SonicWall que monitora em tempo real ciberataques em todo o mundo, até Julho de 2018 mais de 4,5 milhões de ataques de ransomware foram identificados, além de 170 milhões outros ataques envolvendo diversas variantes de malware, tudo isto, apenas no Brasil.

Estes dados alarmantes apontam cenário em que nossas empresas estão inseridas - e naturalmente não exclui o agronegócio, por sua posição estratégica e econômica.

Neste sentido, dada a natureza dos vetores de investimentos em tecnologia, podemos assumir alguns desafios importantes em relação a segurança da informação:

### Ransomware e extorsão através de malware

Ransomware é uma realidade. Um surto de ataques se propaga também em nosso país, pressionando empresas a adotar meios para proteger suas infraestruturas de rede, isto também no agronegócio. Ataques conhecidos como zero-day (dia zero) são uma constante – através de novos códigos maliciosos, ou coquetéis de malware. Sua meta, burlar as frágeis arquiteturas de proteção.

### Indisponibilidade de infraestrutura e sistemas

Ataques modernos podem buscar provocar a indisponibilidade de recursos computacionais por diferentes razões, do sequestro de dados ao ativismo político. Os ataques muitas vezes visam a indisponibilidade não apenas de centros de dados ou servidores, mas, também, de dispositivos inteligentes (IoT) ou dispositivos móveis como smartphones ou tablets e mesmo tags. Os dispositivos usados no campo para capturar de dados, muitas vezes, não contam com camadas adequadas de segurança, aumentando ainda mais o risco para o agronegócio.

### Violação de dados

Considerando-se o papel estratégico do agronegócio, podemos facilmente inferir que as empresas nesse setor são alvo de ataques direcionados. A meta dos criminosos digitais é buscar dados confidenciais vinculados à pesquisa e desenvolvimento. O lucro está no roubo de propriedade intelectual – fonte de diferenciais competitivos para as modernas empresas dentro do agronegócio.



## 5 etapas para manter segura sua empresa no agronegócio

Executivos no agronegócio precisam focar em seus negócios.

Frente às prioridades de investimento e desafios de cibersegurança as empresas no agronegócio precisam repensar sua postura relacionada a segurança de redes.

Nas próximas páginas, especialistas da SonicWall apontam cinco elementos chave para que executivos neste setor tenham menos medo para seguir em seus investimentos para melhorar a sua produtividade e fiquem focados em seus negócios.

## ETAPA 1

# Implemente segurança em camadas

Seu desafio: Reforçar sua defesa contra novas ciberameaças, como ransomware.

Com um crescimento de 400%, ano contra ano, e mais de 4,5 milhões de ataques apenas em 2018, códigos como ransomware já se tornaram uma epidemia digital.

Esses ataques, burlam firewalls incapazes de inspecionar tráfego de internet, incluindo SSL/TLS, verificar potenciais novas ameaças (zero-day) e proteger contra ataques persistentes até uma validação completa de todo o fluxo de dados.

## Sua solução: Implante um Firewall de Próxima Geração

A melhor abordagem para segurança em empresas no agronegócio é adotar Firewalls de Próxima Geração que contam com recursos totalmente integrados através de uma única plataforma e facilitam a administração, e garantem total visibilidade sobre tráfego, além de combinar recursos para melhorar o desempenho de redes como balanceamento de carga, otimização em redes WAN (Wide Area Network). E tudo isto quer sejam redes ecabeadas, remotas, arquiteturas em nuvem ou redes sem fio.





## ETAPA 2

# Estenda a segurança para redes móveis

Seu desafio: Impedir ataques baseados em conexão sem fio

A conectividade sem fio garante hoje para o agronegócio uma série de benefícios, para conectar com velocidade, dados coletados de diferentes maneiras diretamente do campo para laboratórios, áreas administrativas/operacionais, além de apoiar em diversos processos logísticos. No entanto, também abre mais caminhos para diferentes ataques que buscam na fragilidade dos pontos de acesso, uma brecha perfeita para a entrada de códigos maliciosos ou o roubo de credenciais.

Sua solução: Integre recursos de segurança diretamente ao ponto de acesso

Uma abordagem simples para o agronegócio seria trazer as redes sem fio para dentro do perímetro de segurança. Ao fazer isso, as políticas de segurança definidas podem ser aplicadas a usuários sem fio quer sejam em implementações indoor ou outdoor de alto desempenho. A segurança sem fio também deve isolar os funcionários, convidados e uma série de outros perfis para garantir privacidade e confidencialidade de dados. Além disso, os recursos de conectividade e segurança destas redes sem fio, deveriam ser gerenciadas juntamente com as redes cabeadas, sem agregar com isto, complexidade ou custos desnecessários.



### ETAPA 3

## Esteja preparado para o inesperado

Seu desafio: Estar preparado para interrupções não planejadas

Até as redes mais protegidas precisam estar preparadas para eventos inesperados. Para empresas no agronegócio que vêm investindo para automatizar suas operações, adotando dispositivos inteligentes (IoT) ou usando informações em tempo real para melhorar a sua produtividade, passa a ser imperativo adotar tecnologias que permitam gerenciar em tempo real potenciais ameaças e ter recursos para mitigar automaticamente potenciais problemas, quer sejam em centros de dados, redes remotas ou sem fio e mesmo em dispositivos e endpoints.

Sua solução: Estabeleça uma gestão proativa de segurança

As empresas no agronegócio deveriam estar mais focadas em seus negócios e, para isto, deveriam adotar recursos em nuvem para gerenciar também sua infraestrutura de segurança de rede quer sejam cabeadas ou sem fio, através de uma única plataforma de gestão. Além disto, os recursos de segurança devem prever funções de recuperação automática para endpoints e também garantir proteção contra potenciais ameaças avançadas, mesmo aquelas direcionadas contra processadores e outros de hardware comprometidos por códigos maliciosos como Meltdown and Spectre.





#### ETAPA 4

## Simplifique sua infraestrutura de segurança

Seu desafio: Reduzir a complexidade

Em um contexto complexo relacionado a ciberameaças passa a ser fundamental uma postura mais ativa em relação ao tema de segurança, mas que seja factível de ser administrada enquanto você está focado em suportar processos críticos para sua empresa no agronegócio.

Sua solução: Simplifique a gestão de segurança

A segurança com alto desempenho não precisa ser complexa. Os modernos dispositivos de segurança podem facilitar a implementação de recursos e políticas, ajudar na configuração e sobre gerenciamento e na manutenção, usando recursos como interfaces intuitivas baseadas em nuvem e assistentes de configuração fáceis de usar. Não importa o número de localidades remotas, o gerenciamento centralizado ou hospedado pode facilitar ainda mais a administração e, em última análise, apoiar também na redução do custo de propriedade.

## ETAPA 5

# Reduza seu TCO em segurança

Seu desafio: Garantir a segurança de próxima geração dentro do seu orçamento

Empresas no agronegócio, não importa o porte, precisam hoje de recursos avançados de segurança e não podem mais estar alheias aos riscos impostos pela digitalização de processos. Porém, em muitos casos, obter a melhor proteção significa gastar além do orçamento.

O Custo Total de Propriedade, também conhecido como TCO, do inglês, Total Cost of Ownership, compreende não apenas o preço de aquisição de dispositivos de segurança como firewalls, licenças de software, ou a assinatura de contratos de serviços. Mas sobretudo no custo de implementar, usar, gerenciar, manter sua solução ativa e atualizada.

Sua solução: Adote uma plataforma de segurança de rede de fim a fim

Reduza seus custos de hardware, configuração, operações e despesas gerais de manutenção consolidando várias ferramentas de segurança em uma única arquitetura para melhorar a sua gestão. Esta solução deve garantir baixo TCO e ir além de recursos básicos de firewall, e entregar também filtro de conteúdo, prevenção contra invasões, antispymware, antimalware, e que esteja integrada à segurança de endpoints, aplicações Web, em redes cabeadas, sem fio, remotas, tudo através de recursos em nuvem.





## Conclusão

O agronegócio não pode estar alheio às **ciberameaças** - tampouco devem investir mais do que o necessário em tecnologias que não tenham relação direta com seus processos de negócio com a transformação digital de forma ampla para melhorar a sua produtividade.

Segurança avançada é uma exigência para empresas que buscam se manter competitivas dadas a diversas implicações, mas ter acesso a tudo isto deve possível com recursos integrados e através de uma abordagem simples. Propostas de valor que a SonicWall vem trazendo para o mercado há mais de 27 anos em todo o mundo, e mais de 17 anos no Brasil.

Nós acreditamos que todo este cenário de ciberinsegurança que vivemos pode também representar uma oportunidade para as empresas neste setor prosperarem.

Por meio de sua rede de parceiros – empresas com profissionais treinados e capacitados em segurança da informação – a SonicWall atende o agronegócio em sua localidade. Isso inclui serviços e soluções de segurança sob medida para os seus negócios, sem pagar mais por isso.

A SonicWall acredita que mais segurança é a garantia de menos preocupações para melhores negócios.

Conheça mais sobre as soluções de segurança da SonicWall e sua operação no Brasil em:

[www.SonicWall.com/pt-br/](http://www.SonicWall.com/pt-br/)

## About Us

Over a 27 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.

Refer to our website for additional information.

[www.sonicwall.com](http://www.sonicwall.com)

## © 2018 SonicWall (R). ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.