



# ThreatPROTECT

Compare continuamente os dados de ameaças externas com relação a suas vulnerabilidades internas e identifique os ativos de TI que exigem correção imediata

Tudo que você precisa para ter segurança e conformidade contínuas

Adquira o Qualys TP como um aplicativo independente ou como parte da plataforma de nuvem da Qualys. É uma plataforma de segurança e conformidade em que é possível detectar, defender e proteger todos os seus ativos globais de TI onde quer que eles estejam.

O Qualys Security and Compliance Suite inclui as valiosas ferramentas a seguir:

- AV** – AssetView
- VM** – Vulnerability Management
- CM** – Continuous Monitoring
- TP** – ThreatPROTECT
- PC** – Policy Compliance
- SAQ** – Security Assessment Questionnaire
- PCI** – PCI Compliance
- WAS** – Web App Scanning
- WAF** – Web App Firewall
- MD** – Malware Detection
- SEAL** – Qualys Secure Seal



O Qualys ThreatPROTECT (TP) é um serviço em nuvem que compara os dados de ameaças externas com relação às vulnerabilidades internas de uma organização e permite que os profissionais de TI priorizem automaticamente o trabalho de correção, como implementação de patches e redução de riscos.

Tentar acompanhar as divulgações de vulnerabilidades, um volume de milhares ao ano, é uma tarefa extraordinariamente difícil. Até as melhores equipes de segurança das informações podem ficar sobrecarregadas tentando descobrir qual dessas ameaças externas representa o maior perigo para seu ambiente de TI em um determinado momento.

O ThreatPROTECT identifica os ativos de TI com maior risco, eliminando o trabalho de adivinhar quais itens devem ter patch primeiro. Com um painel de controle intuitivo, feed de informações contra ameaças em tempo real e um mecanismo de pesquisa avançado, o ThreatPROTECT proporciona uma visão "geral" abrangente e contextual de seu dinâmico panorama de vulnerabilidades.

Nunca mais deixe perigosas lacunas abertas inadvertidamente por semanas, meses e até mesmo anos. Priorize a correção de vulnerabilidades de maneira inteligente, deliberada e tática com o ThreatPROTECT.



## Benefícios:

Domine a sobrecarga de dados de vulnerabilidades e recupere o controle sobre a priorização de correções.

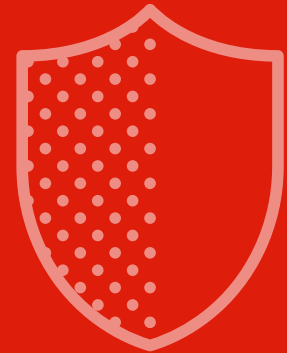
Baseie as ações de correção na análise contínua e precisa de ameaças correlacionadas, e não em suposições nem agendamentos arbitrários de aplicação de patch.

Poupe tempo e faça o melhor uso de seus recursos de aplicação de patch.

Obtenha alertas sobre vulnerabilidades antigas e de baixo risco que repentinamente se tornam perigosas.

Veja todo o seu inventário de ativos de TI e as vulnerabilidades "de modo geral" e se aprofunde nos detalhes do dispositivo e do software.

Aproveite os benefícios da nuvem da Qualys, como não precisar instalar nem manter o ThreatPROTECT.



## Principais recursos:

### Feed de informações contra ameaças em tempo real

Acorde todos os dias e veja uma lista de vulnerabilidades que representam risco imediato para seus negócios.

- Mantém as organizações atualizadas sobre as mais recentes divulgações e anúncios de vulnerabilidades.
- Com recursos avançados de correlação, exibe a quantidade de ativos de TI que foram afetados pelas divulgações.
- Permite que você se aprofunde e obtenha detalhes de determinadas vulnerabilidades e dos ativos de TI afetados.
- Possibilita o ajuste da lista de feeds filtrando e classificando itens de acordo com uma série de critérios.

### Painel de controle dinâmico

Visualize ameaças críticas para seu ambiente.

- Exibe toda a postura de ameaças rapidamente.
- Fornece exibições dinâmicas e personalizáveis com estatísticas específicas, como ativos com vulnerabilidades zero-day ativas.
- Possibilita clicar e acessar mais informações sobre os ativos identificados como vulneráveis.

### Mecanismo de pesquisa

- Proporciona uma ferramenta avançada para procurar ativos e vulnerabilidades específicos proativamente.
- Permite criar consultas específicas com múltiplas variáveis e critérios, como: **classe do ativo, tipo de vulnerabilidade e sistema operacional.**
- Permite que os resultados da pesquisa sejam classificados, filtrados e refinados ainda mais.
- Possibilita salvar consultas e transformá-las em exibições permanentes do painel de controle.

## Folha de dados: Qualys ThreatPROTECT

The screenshot shows the 'Live Feed' interface with the following alerts:

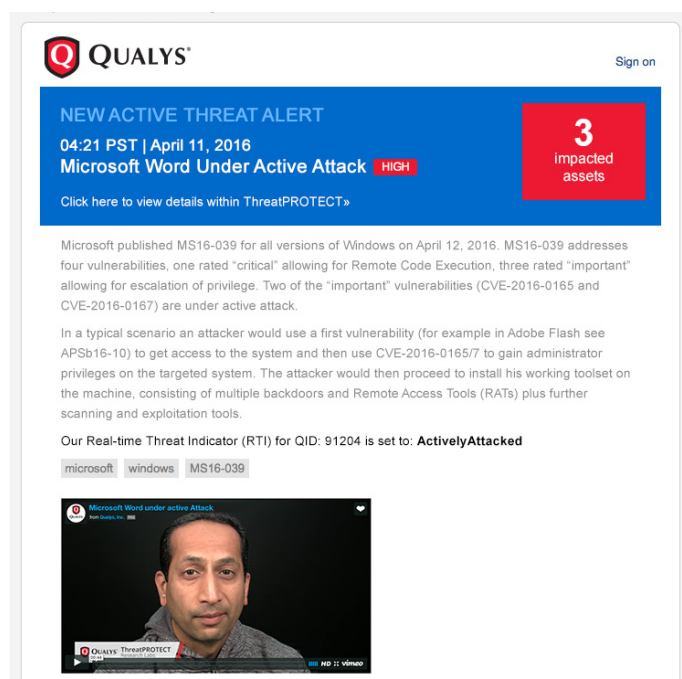
- Analysis of RIG Exploit Kit weaponizing CVE-2016-0034** (MEDIUM) - April 26, 5 Impacted Assets. Description: Exploit kit authors often update the capabilities of their exploit kits by adding support for new vulnerabilities so that they can compromise and install malware or ransomware on even more machines. As part of the ThreatPROTECT research team, I analyze exploit kits to keep track of the latest vulnerabilities being incorporated into them. Back in...
- Accellion FTA Vulnerabilities** (HIGH) - April 21, 0 Impacted Assets. Description: Security researcher Orange recently managed to gain access to a file transfer server at Facebook. He used a set of vulnerabilities that he found in the product that provides the service: the Accellion File Transfer Server (FTA). He notified Facebook under their bug bounty program and was awarded US\$ 10,000. Accellion addressed...
- Microsoft Windows under active attack** (HIGH) - April 11, 3 Impacted Assets. Description: Microsoft published MS16-039 for all versions of Windows on April 12, 2016. MS16-039 addresses four vulnerabilities, one rated "critical" allowing for Remote Code Execution, three rated "important" allowing for escalation of privilege. Two of the "important" vulnerabilities (CVE-2016-0165 and CVE-2016-0167) are under activ...
- Adobe Flash Player under new 0-day attack** (HIGH) - April 04, 15 Impacted Assets. Description: Adobe announced that a new version of their Flash Player product is expected to be released this week. The new version will address CVE-2016-1019, a critical vulnerability that is currently being exploited in the wild. However, if you are current with your Flash player patches you are protected. If you have the newest Flash player installed...
- Adobe Flash partial 0-day patched in OOB release** (HIGH) - April 04, 15 Impacted Assets. Description: Adobe addressed a partial 0-day vulnerability in its Flash player with a software release on April 7, 2016. The new version of Flash fixes 24 vulnerabilities, with CVE-2016-1019 under active attack through the Magnitude Exploit Kit. The vulnerability is a partial 0-day because in the newest version of Flash a mitigation strategy introduced by Adob...

## Principais recursos – continuação:

### Recursos de alerta e visualização

Avalie seu progresso e os esforços de correção com análise de tendências em tempo real e obtenha alertas quando novas ameaças ativas surgirem em seu ambiente.

- Gera relatórios, gráficos e tabelas.
- Permite exibi-los no painel de controle e compartilhá-los com colegas.
- Envia notificações alertando quando limites e parâmetros predefinidos forem atingidos e quando ventos pré-determinados ocorrerem.



### Informações abrangentes sobre vulnerabilidades de fontes internas e externas

Os engenheiros de segurança da Qualys validam e classificam novas ameaças constantemente.

- Aproveita os dados de ameaças dos laboratórios de pesquisa da Qualys e de parceiros e fontes externas, inclusive Core Security, Exploit Database, Immunity, TrendMicro, VeriSign iDefense.
- Classifica esses pontos de dados de indicadores de ameaças em tempo real (RTI, Real-Time Threat Indicator), como ataques e exploits, em categorias mais exatas, ajudando a priorizar a correção com mais precisão:

- |                             |                         |
|-----------------------------|-------------------------|
| - Zero day                  | - Grande perda de dados |
| - Exploit público           | - Negação de serviço    |
| - Ativamente atacado        | - Sem patch             |
| - Alta movimentação lateral | - Malware               |
| - Exploit fácil             | - Pacote de exploit     |

Para obter uma versão de avaliação gratuita do Qualys WAF válida por sete dias, acesse [qualys.com/freetrial](http://qualys.com/freetrial)

*Não há nada para instalar nem fazer manutenção*

## Sobre a Qualys

A Qualys, Inc. (NASDAQ: QLYS) é pioneira e principal provedora de soluções de segurança em nuvem e conformidade com mais de 8800 clientes em mais de 100 países, sendo que a maioria deles figuram na Forbes Global 100 e na Fortune 100. As soluções da Qualys ajudam as organizações a simplificar as operações de segurança e reduzir o custo da conformidade oferecendo inteligência de segurança crítica sob demanda e automatizando o espectro completo de auditorias, conformidade e proteção para sistemas de TI e aplicativos web. Fundada em 1999, a Qualys estabeleceu parcerias estratégicas com os principais provedores de serviços gerenciados e organizações de consultoria. A Qualys é membro fundador da Cloud Security Alliance. Para obter mais informações, acesse [www.qualys.com](http://www.qualys.com).



**Qualys, Inc. – sede**  
 1600 Bridge Parkway  
 Redwood Shores, CA 94065 USA  
 T: 1 (800) 745 4355, [info@qualys.com](mailto:info@qualys.com)

A Qualys é uma empresa com escritórios pelo mundo. Para encontrar um escritório perto de você, acesse <http://www.qualys.com>