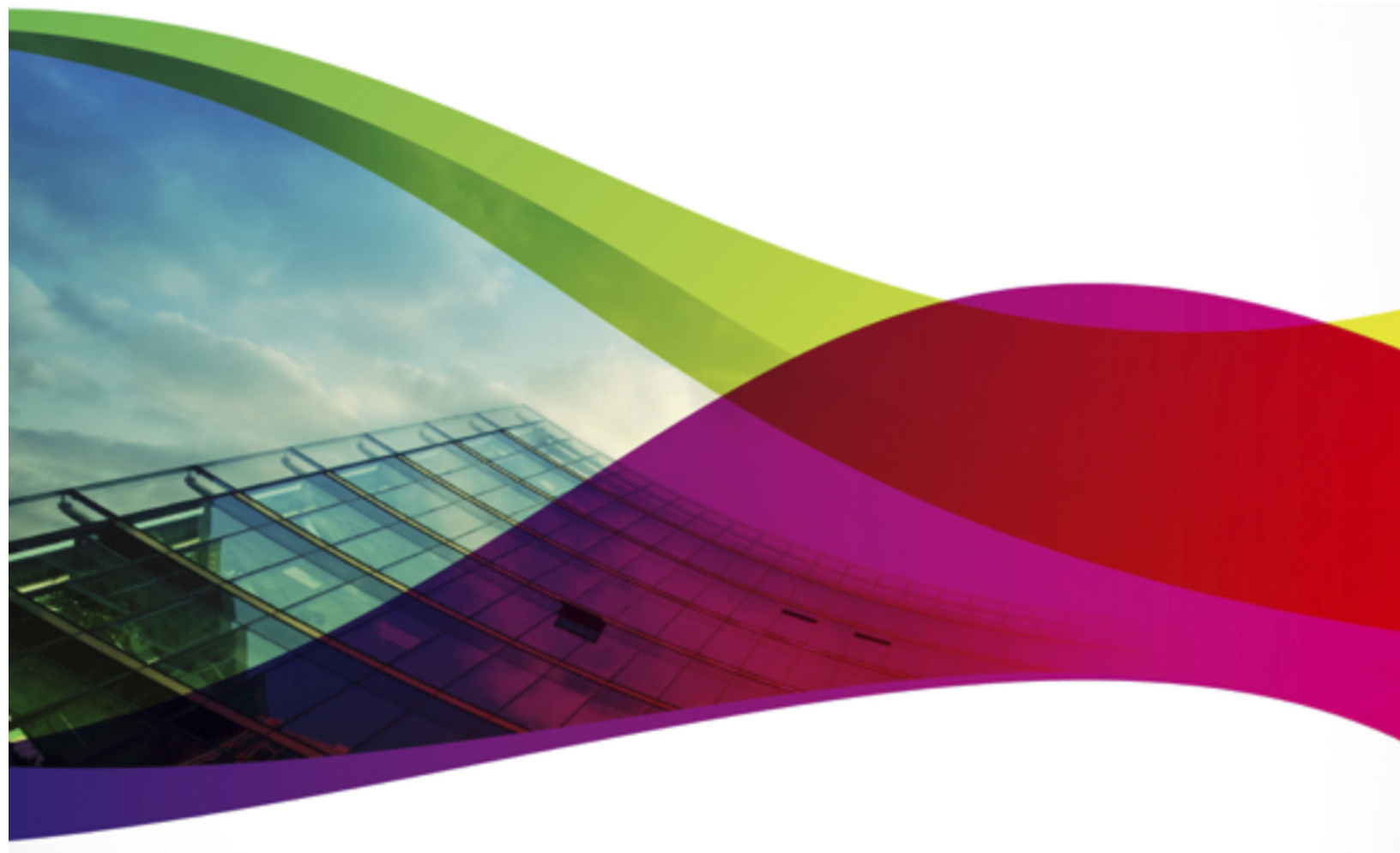


# SAMPLE REPORT

## OfficeScan Best Practice Guide Security Compliance

Prepared for:  
Customer Name: EXAMPLE

Created on: October, 2019



## Contact Details

### Trend Micro Account Manager



[email@trendmicro.com](mailto:email@trendmicro.com)

## Document Conventions

### Severity Classifications:

-  Vulnerability
-  Critical
-  Medium
-  Low
-  Enhancement

### Object Types:

-  Workstation
-  Server

### Data Retention:

All OSCE client specific details as well as the Extraction tool archive will be removed from the autonomous system after 45 days of creating the report.

# High-level Executive Summary

Overall Results for: example.example1.net

OfficeScan Server: XG - SP 1, Build 5261 [EN] (Release date 2018/11/29)

This high-level summary is intended to provide an overview of the current status of your OfficeScan deployment compared with the Trend Micro recommendations of Best Practices. Detailed instructions, business impacts and references can be found in the individual sections further down in the report.



## Summary

Platforms	Total	Online	Offline	Compliance Rating	
OfficeScan Server				75%	●
Desktop Agents	700	669	31	38%	●
Server Agents	31	31	0	43%	●
	731	700	31		

## Release Distribution

Release description	Date	Workstations	Servers
XG Service Pack 1	201/--/--	700	31

## Advanced Feature Compliance

Module Name	Average Compliance	%	Fully Compliant Agents	%
Smart Scan (File Reputation Services)	<div><div></div></div>	100	<div><div></div></div>	100
Real-Time Scan	<div><div></div></div>	50	<div><div></div></div>	0
Web Reputation	<div><div></div></div>	50	<div><div></div></div>	4
Suspicious Connection Service	<div><div></div></div>	100	<div><div></div></div>	100
Behavior Monitoring	<div><div></div></div>	67	<div><div></div></div>	0
Predictive Machine Learning	<div><div></div></div>	0	<div><div></div></div>	0
OfficeScan Agent Self-protection	<div><div></div></div>	100	<div><div></div></div>	100
Device Control	<div><div></div></div>	50	<div><div></div></div>	0

## Key Findings

- The Security is affected by 2 Vulnerabilities and 7 Critical issues (See Hotfix 5325 from 2019/03/13).
- A newer OfficeScan Server version is available. Upgrade to receive the most up-to-date protection

# Table of Contents

1. [Report Overview](#)
2. [OfficeScan Server Compliance](#)
3. [Site Compliance Reports](#)
  - 3.1. [OfficeScan Agent Policy Compliance](#)
4. [Trend Micro Apex One™ Upgrade Checklist](#)
5. [Appendix](#)
  - 5.1. [Available Hotfixes/Patches by Severity](#)
  - 5.2. [Recommended Security Settings for OSCE XG Service Pack 1](#)
    - [Smart Scan \(File Reputation Services\)](#)
    - [Real-Time Scan](#)
    - [Web Reputation](#)
    - [Suspicious Connection Service](#)
    - [Behavior Monitoring](#)
    - [Predictive Machine Learning](#)
    - [OfficeScan Agent Self-protection](#)
    - [Device Control](#)

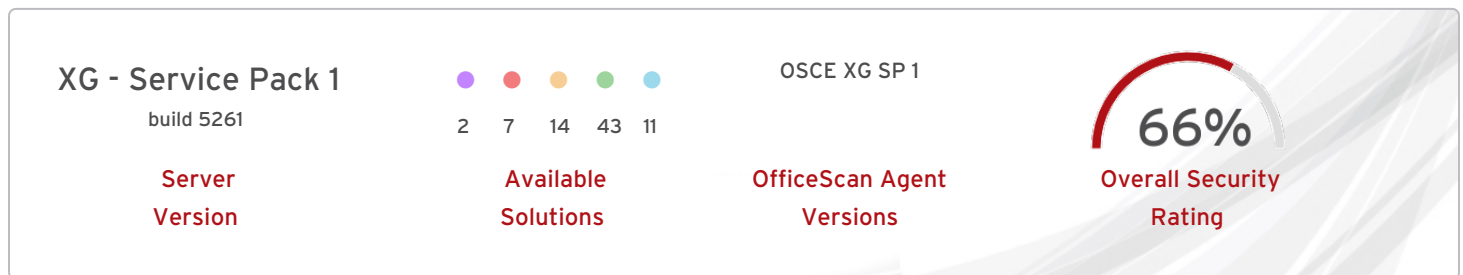
# 1. Report Overview

The primary objective of this report is to outline the current status of endpoints protected by OfficeScan and make recommendations specifically targeted at increasing the overall security posture for your implementation. This report provides the following information:

- Recommendations about how to improve the network security provided by OfficeScan.
- An overview of the currently deployed OfficeScan agent versions.
- An assessment of the current OfficeScan server build compliance and the availability of hotfixes, patches, or enhancements.
- An overview of the protected operating systems.

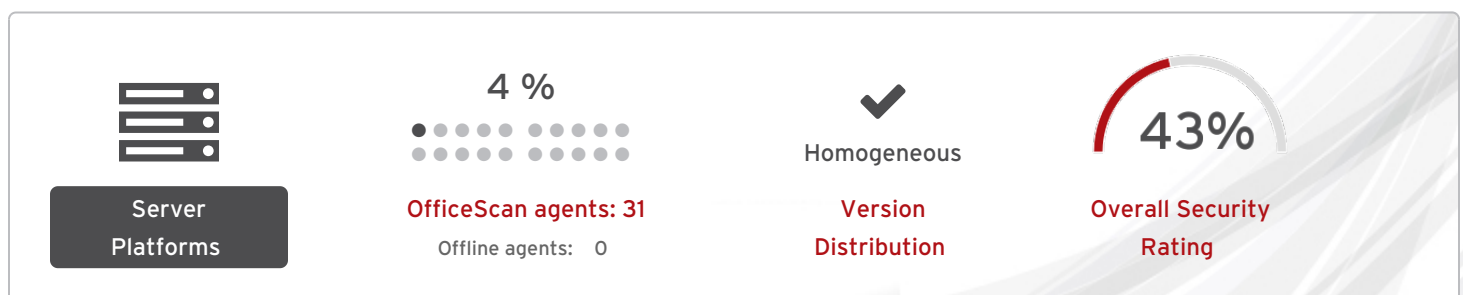
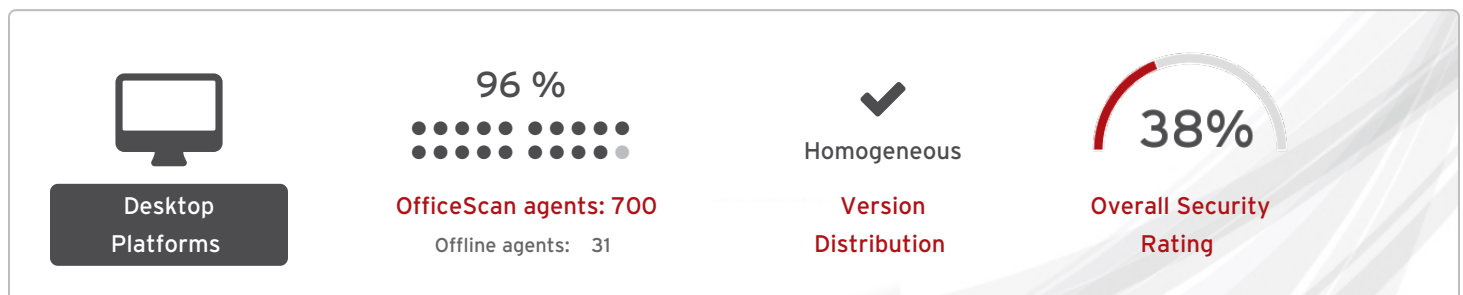


## OfficeScan Server Details



## OfficeScan Agent Details

Total endpoints: 698



Each module may consist of multiple conditions for which you can find the details in section "Security Compliance Overview".

### Smart Scan (File Reputation Services)

Fully compliant agents: 698/698 (100%)

OfficeScan agents using Smart Scan leverage light-weight patterns and cloud reputation queries to provide the same protection provided by conventional anti-malware and anti-spyware patterns. Smart Scan agents perform scanning locally and if the local scan is unable to determine the risk of a file, a query is sent to Smart Protection sources. Smart Scan agents cache the query results to improve scan operations.



### Real-Time Scan

Fully compliant agents: 0/698 (0%)

Real-time Scan is a persistent and ongoing scan. Each time a file is received, opened, downloaded, copied, or modified, Real-time Scan scans the file for security risks.



### Web Reputation

Fully compliant agents: 31/698 (4%)

Web reputation technology tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes, and indications of suspicious activities discovered through malware behavior analysis. When a user attempts to access a website, the OfficeScan agent queries a smart protection source to ascertain the risk level of the content.



### Suspicious Connection Service

Fully compliant agents: 698/698 (100%)

The Suspicious Connection Service manages the User-defined and Global IP C&C lists, and monitors the behavior of connections that endpoints make to potential C&C servers.



### Behavior Monitoring

Fully compliant agents: 0/698 (0%)

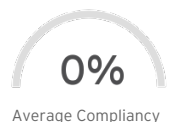
Behavior Monitoring constantly monitors endpoints for unusual modifications to the operating system or installed software. Through use of Malware Behavior Blocking and Event Monitoring, Behavior Monitoring protects endpoints against unconventional threats, such as ransomware attacks.



### Predictive Machine Learning

Fully compliant agents: 0/698 (0%)

Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis or behavioral process and script analysis to detect emerging unknown security risks.



### OfficeScan Agent Self-protection

Fully compliant agents: 698/698 (100%)

OfficeScan agent self-protection provides ways for the OfficeScan agent to protect the processes and other resources required to function properly. Self-protection helps thwart attempts by programs or actual users to disable anti-malware protection.



### Device Control

Fully compliant agents: 0/698 (0%)

Device Control regulates access to external storage devices and network resources connected to endpoints. Device Control helps prevent data loss and leakage and, combined with file scanning, helps guard against security risks.

