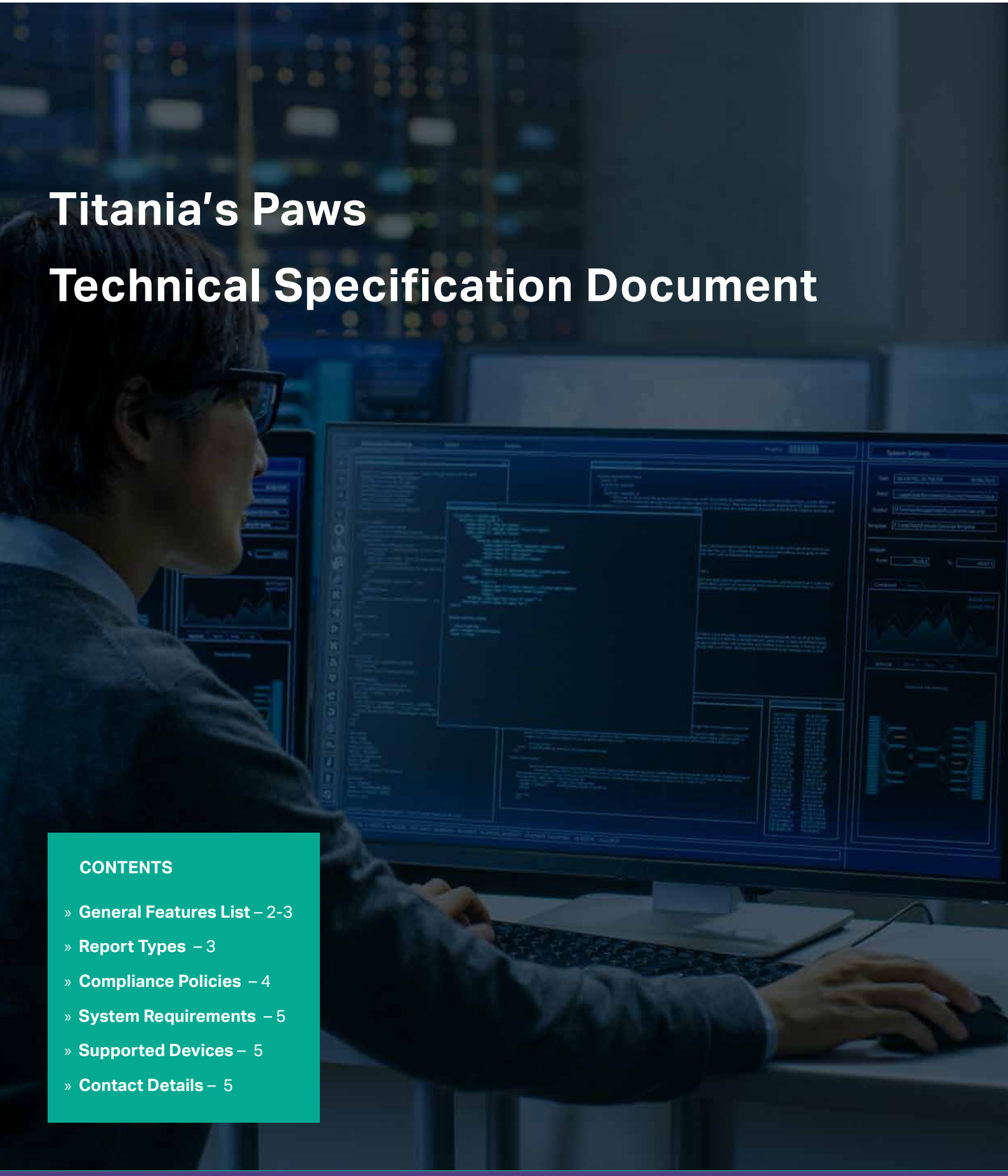
TITANIA
PAWS

Titania's Paws
Technical Specification Document



CONTENTS

Why the world's most secure networks use Titania Paws

General Features List

Feature	Benefit
Reports are generated in seconds	This means that you can get results instantly and act fast.
Competitive per device pricing model	This means that you can purchase the right size license for your network and grow it with your network.
Paws Policy Editor Using the data collector you can create your own policy to audit against. You can also edit the pre-defined policies.	This means that no matter what policy you want to audit you can do this with Paws, offering ultimate flexibility.
Pre-defined compliance policies	Using our pre-defined policies you can instantly check your security against industry standards, helping to become compliant and avoid fines and breaches.
Paws Data Collector This is an executable file that can be put onto the machine being audited to extract the configuration, leaving no footprint behind.	Although you can do this across the network, the option of not connecting to the network means that it can be used in locked down environments and does not leave anything that could be dangerous behind.
Fast installation & multi-device activation The software can be downloaded and installed in minutes on multiple machines.	This is perfect for multi-auditor teams where there are several people using the same license. It is also useful for pen testers who go to multiple sites.
Easy to understand and use Paws reports are written in plain English, making them easier to understand. They include graphs and summaries. Help guidance is offered throughout the software to explain terminology and functions.	Easy to understand reports with lots of explanation means that users can operate the software straight away and don't need to waste time contacting us for support. Graphs and summaries mean it is easy to report findings to non-technical managers.
Multiple export options Individual tables can be saved and distributed.	This helps when actioning the report. By saving sections of the report into CSV for example, network security managers can have parts of the report actioned easily without having to distribute the entire report.
New report User Interface	We have improved the usability of the tool so that it is easier for you to drill down into the specific sections of the report, while still being able to export the entire report if you want to. This makes it easier for you to work your way through the findings, especially when checking against multiple policies or on lots of different machines.
Self Certification Auditing Type	We have added a new auditing type, self-certification. These are questionnaire type policies that, where appropriate, we have made recommendations to suggest the answer. These are available through an extra bolt-on purchase on a license. The built-in self certification policies are Cyber Essentials and DCPP CSM for the MOD.

Feature	Benefit
Save / reload reports	We understand that often a compliance audit will not be completed in one sitting, you may need to come back to it later on. With Paws you are able to save a report at any point and reload it into the software, picking up where you left off. By switching on a setting, every time you launch Paws it will pick up the last report you saved, but of course if you want to work on a new one, then simply generate a new report.
Re-run specific checks	You are now able to re-run a report on specific checks, policies or devices rather than the entire report. This is perfect for when you are fixing issues as you go. You can instantly regenerate the report as you make changes, without having to re-run every check on every device, saving you time.
Overriding check results	New functionality means that you are able to override the result of a check in any policy you are auditing against. For example, if you feel the you may have good reason to deviate from the policy you can forcibly pass a check that may have otherwise failed.
Improved reporting performance	Enhancements we have made have helped to make the generating of reports even faster, so you can act fast on securing your network.
Event logging	There is an option to turn on event logging with Paws. This helps you to integrate the Paws findings into other systems (such as SIEM) that you may have, and make it easier to manage the view of the report output in the context of everything else on your system.
Demo mode	If you don't have a license, you can load the demo file to see a complete report for all policies against a set of dummy devices. This means that users can demonstrate the product to colleagues without having to use their own, potentially sensitive information.

Report Types

» **Titania's Policy Editor** – Paws Policy Editor lets you quickly create your own security audits from scratch (or by editing pre-defined polices). Customized reports can be generated in seconds. Less time auditing, more time securing your systems.

» **Configuration Report** – A detailed report showing your machine configuration. This report gives you a quick and clear view of your current device settings.

Compliance Policies / Industry Standards

Our customers use Paws to quickly gain insight and validation against a range of industry standards. The compliance reports types listed below are the pre-defined policies within the software.

	The CIS (Center for Internet Security) benchmarks are a set of consensus-based security configuration guides that are gaining an important role in shaping policies and decisions. Developed and accepted by government, industry and academia, the CIS standards now encompass compliance requirements of other industry policies such as FISMA, PCI, HIPAA and more. Paws can audit your devices in line with the CIS baseline and produce reports externally certified by CIS.
NIST	The purpose of the United States Government Configuration Baseline (USGCB) initiative is to create security configuration baselines for Information Technology products widely deployed across the federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate. The USGCB is a federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain an effective configuration settings focusing primarily on security.
	Detailed system reporting against the U.S. Military DISA STIG Checklists. Paws is favoured by many government and defence agencies because reports can be generated securely offline and scaled up to audit any number of devices.
PCI DSS	This is an audit against the Payment Card Industry policy. If you need to comply with this standard, the report will quickly complete the automatable checks, explain where and why you have passed or failed and offer advice to help you become compliant.
	Cyber Essentials is a Government-backed and industry supported scheme to guide businesses in protecting themselves from cyber threats. It is derived from years of research on business breaches which resulted in practical, easy to implement actions removing up to 80% of your cyber risk. Paws will audit your devices against the standard, checking automatically against automated checks and supplying interactive questionnaires for those checks requiring human input, so you can be assured of 100% compliance.
	The Defence Cyber Protection Partnership (DCPP) is a joint MOD / Industry initiative that was established in 2013. The DCPP is tasked with improving the protection of the defence supply chain from the cyber threat. Alongside MOD, the DCPP is made up of 13 defence primes; 2 trade associations ADS (Aerospace, Defence and Security) and techUK representing small and medium sized enterprises (SMEs); the Department for Culture, Media and Sport; the Communications Electronics Security Group (CESG) and the Centre for the Protection of National Infrastructure (CPNI).
	The U.S. National Security Agency (NSA) security guidelines are trusted all over the world as an authority on information security. With input from many security experts, this offers useful insights into system configuration vulnerabilities.
OVAL	Improve security in three key areas: system information, specific machine states and assessment reporting. OVAL information assurance metrics include data on publicly available security issues (often targeted by cyber criminals). This report helps you quickly find and plug these holes.
SANS	The SANS institute is a trusted industry body and provider of training for security professionals. Their policy is used all over the world as a security benchmark, why not use this report to see how your defenses stack up?
NERC CIP	The NERC standard provides requirements for Critical National Infrastructure Protection (CNIP). This standard is mandatory for CIP providers in the U.S.A. and a global benchmark for protecting many critical networks.

System Requirements

OS		
Requirements	Microsoft Windows 7 or above (Server 2008 R2 or above) 400MB disk space 2GB memory	GNU/Linux (RHEL, Fedora, CentOS) 600MB disk space 2GB memory

Supported Devices

Supported Devices for Configuration Reporting
RedHat
CentOS
Fedora

Supported Devices for All Report Types
Windows 10, 8 (8.1), 7, Vista & XP
Windows Server 2016, 2012 R2, 2012, 2008 & 2003

Supported Devices for STIG
Red Hat 7

Contact: enquiries@titania.com | +44 (0)1905 888 785 | www.titania.com