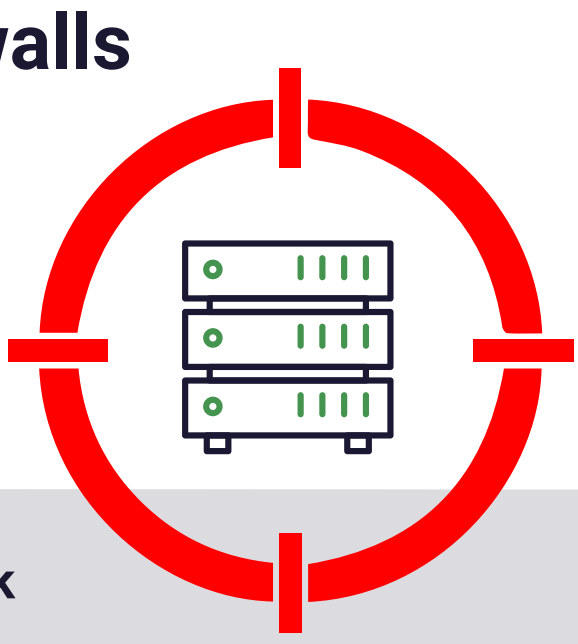
TITANIA Assured Accuracy | merlin cyber

Every day U.S federal agency routers, switches and firewalls are under cyber attack



As critical vulnerabilities have been found in network switches used in millions of enterprises this year, **it's a case of when, not if, a network will be attacked.**

All federal respondents feel their network security tools are meeting security and compliance requirements

71% of federal respondents reported that their network security tools enabled them to categorize and prioritize compliance risks very effectively

65% had partially-automated, full measurement and reporting of KPIs

However, compliance does not equal security

51 network misconfigurations were identified by federal agencies over the past 12 months

4% of identified network misconfigurations could have led to a **serious breach of security**

Why are serious threats still bypassing U.S. Federal Government network security controls?

0% of federal respondents assess their network routers and switches

0% checked firewalls for misconfigurations more frequently than **bi-monthly**

12% of government respondents assessed firewalls **bi-monthly**

59% of government respondents said they assess the configuration of network devices on an **annual basis**

88% of federal respondents **rely on compliance** to deliver security

3 things you can do to eliminate the threat of configuration drift from taking down networks

1

Don't neglect the assessment of routers and switches.

Monitor the configuration of all network devices, particularly routers and switches. Routers and switches are as essential as firewalls and, if not regularly assessed, will continue to serve as an exploitable foothold for malicious actors to gain unauthorized network access.

2

Catch network misconfigurations when they happen by implementing continuous configuration management.

If you are assessing the configuration of network devices annually, then you must be comfortable with having malicious actors sitting inside your network for up to 364 days. Closing the time gap to near zero by implementing continuous configuration takes the risks associated with configuration drift out of your risk equation.

3

Bake continuous network device monitoring into regulatory compliance requirements.

Continuous monitoring of all network devices is fast becoming a requirement – we are seeing this requirement being written into PCI and other standards. Since the Federal Government largely implements security controls based on compliance requirements, this would be a very welcome, needed driver to help close security gaps introduced by exploitable misconfigurations.

Download the report into the impact of exploitable misconfigurations on network security within US Federal organizations to learn more

Download now >