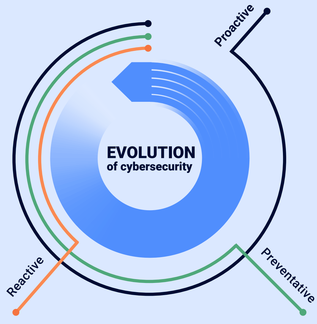
TITANIA

OMDIA
Brought to you by Informa Tech

Emerging best practice in the use of proactive security solutions

Organizations now investing in proactive security over preventative and reactive approaches, in the shift towards more pre-emptive attack surface exposure management...



Proactive

is top cybersecurity goal for organizations in the next 12-24 months

Research conducted by Omdia has shown that while the cybersecurity industry has clung to the "assume breach" mantra with its preventative and reactive solutions, organizations are awakening to a smarter strategy: proactively understanding attack surfaces, mapping attack paths, and plugging vulnerabilities to prevent breaches.

Respondents reported increased investment in proactive security solutions over preventative and reactive measures during the last twelve months. Preventative and reactive solutions will not disappear, but organizations are shuffling their spending priorities and looking for the better ROI that proactive security solutions promise to deliver.

3 most common priorities

Reduce the opportunity for threats with proactive security

Focus on zero trust network segmentation and dynamically analyzing exposure to MITRE ATT&CK TTPs

Reduce mean time to remediate known vulnerabilities

Automatically determine the network's most exploitable risks and prioritize remediation to shut them down

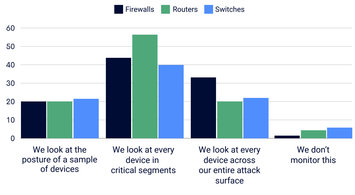
Minimize attack surface with proactive configuration drift monitoring

Get immediate visibility of each configuration change - planned and unplanned - and assess for potential indicators of compromise

Top challenges to overcome

Many organizations have limited visibility into their network assets, with a significant portion only monitoring a sample of devices or devices in critical segments rather than every device across their entire attack surface.

Limited visibility



Minimal proactive monitoring

TITANIA OMDIA
Brought to you by Informa Tech

Download the full research report

titania.com/proactive-security-solutions