# 5 key requirements for a secure 5G network


- AT&T currently sees 11 billion security incidents each day
- As architecture evolves to support 5G networks it will open more vulnerabilities
- A multi-layered and proactive approach is vital to minimize these threats

The security challenges facing service providers are set to soar with the development of 5G networks. That's why many will choose to buy-in these capabilities via an IaaS model. If that's the case, there are several key features operators should look for to ensure maximum protection.

Service providers are facing a never before seen array of cyber threats. And as your architecture evolves to support 5G networks it will only open more doors for the bad guys. Unlike 4G and previous generations, 5G will support specialized use cases like e-health and connected cars. Security in these scenarios could be a matter of life and death.

In addition, network slicing will require new and dynamic network security for each slice and each individual customer. Plus, there'll be a growing DDoS threat from RAN-side 5G devices that have been compromised.

So what's the answer? The costs and expertise required can be vast. Here are the five main features to focus on:

**Threat prevention** can minimize those basic issues that still account for many security incidents. Consider firewalls to protect your network from external networks. And access controls to minimize user-based risk. Intrusion detection and prevention tools can also help by blocking basic security threats.

Your security architecture must evolve as you move to 5G. This whitepaper offers a roadmap for your journey

**Advanced malware** must be stopped and fixed. For this, you need to go beyond signature-based tools to spot the stuff designed to evade basic filters. Behavior-based checks on endpoints, possibly using sandboxing, are important. And once a threat has been detected, you need to be able to remove all instances of it on the network, and block it going forward.

**Anomaly detection** uses packet capture, big data, and machine learning to identify threats not spotted by basic filters. When embedded into network switches and routers it's far more effective, as it turns those devices into security sensors.

**DNS intelligence** is important, as this is a major threat vector today. There's great value in tools which monitor DNS activity and protect against anything malicious. But this is extremely expensive and resource-intensive to develop in-house. So look for an expert provider who can help.

**Threat intelligence** should be at the heart of any effective 5G security strategy. Service providers must look for vendors which profile hackers to better understand their efforts. Try and get intelligence from the widest range of sources possible. Ensure your provider only offers actionable intelligence and that it's sent to you rapidly.

Security threats are only going to accelerate as 5G networks become a reality. AT&T sees 11 billion incidents each day currently. But it predicts this will rise to five billion every 10 minutes in the future.

That's why service providers must plan now for the future. And remember, the first step towards control is network-wide visibility.

https://www.cisco.com/c/m/en_us/network-intelligence/service-provider/digital-transformation/secure-5g-network.html