CHECKLIST

How an Intelligent Network Can Unburden IT Teams

Today's networks are expected to do more than deliver connectivity and bandwidth. To optimize performance and enable additional functionality, a network needs to be intelligent. The more intelligent the network, the better it will perform, and the more tasks it can offload from IT teams. The following list highlights five important ways that intelligence can be built into the network to make things easier on those running it.

☑ Run Initial Startup and Configuration With Ease

Zero-touch provisioning. Having intelligence built into the equipment that at its initial boot can check for and pull configuration with no additional work for IT is a major benefit. This functionality is usually called zero-touch provisioning. Automatic configuration makes installing equipment a breeze and cuts down on expensive on-site resources. As an organization continues to grow, sites can be templatized for easy handling of a distributed installation base.

☑ Automatically Onboard Users and Devices

Automated onboarding. This can be thought of as initial setup for the end-user devices. Intelligence at the edge that puts devices into the correct context simplifies security and improves overall user experience. It's valuable for this capability to be embedded into the equipment to ensure that all policies are a match to existing LAN policies. The more cohesion across configuration options, the easier long-term management becomes. As the number of Internet-of-Things (IoT) and end-user devices continues to rise, more and more time is saved by having intelligent mechanisms to onboard them without manual intervention.

☑ Get Insight and Recommendations

Artificial intelligence (AI) and machine learning (ML). Watching larger trends and understanding when things have gone awry is a perfect example of the sort of thing that computers can do very quickly, but people cannot. Having an AI/ML resource at the network heart that can take information from throughout the installation ensures that trend evaluation is comprehensive and accurate. From there, specific actionable recommendations can be made to avert disruption, or for improvement. The wider the array of resources (LAN, WLAN, firewalls, SD-WAN, etc.) that AI/ML can take inputs from, the better the correctional steps will be.

☑ Auto-quarantine Corrupted Devices

Auto-quarantine. With malware incidents on the rise, having the ability to watch devices and know when they have been compromised improves security of the network (and thus overall performance) considerably. Intelligent systems can look for indicators of compromise (IOCs) and then take automated actions when it becomes apparent that a device is infected. Installations that leverage a large number of IoT devices are especially vulnerable as these devices often have weak onboard security and it can be particularly difficult for a human to "see" when such a device is misbehaving. IOC intelligence can detect and remediate the issue before the network is impacted.

☑ Prioritize Traffic

Application awareness. All traffic on the network is not of equal importance to the organization. Business-critical traffic (virtually by definition) needs to be treated differently than other traffic. Having embedded application awareness within the network allows traffic to be handled as desired, even as conditions change within the network. This keeps business moving productively regardless of traffic load or number of attached devices.

Summary

A network that has built-in intelligence cuts down on the tactical tasks that IT needs to perform daily, freeing time for corporate initiatives and ensuring that digital acceleration continues as planned.

www.fortinet.com

January 12, 2022 12:23 AM
1410153-0-0-EN