ManageEngine
DDI Central

DDI Endpoint Integration datasheet

The devices joining an organization's network need to be monitored. Also, their data needs to be analyzed for a contextualized view of insights such as system info, patch status, and vulnerabilities, which network admins need to know and have an eye on them. Without the information, admins would be unsure if the devices connecting are reliable and secure.

Manage Engine's DDI Central, with the integration of Endpoint Central, lay outs deeper visibility over real time data of the DHCP leases. This helps organizations diagnose potential cybersecurity risks and troubleshoot them to prevent further damage in the network infrastructure.

Detailed view over devices

The DDI integration with Endpoint Central brings in endpoint data, like OS, device type, memory, disk usage, manufacturer, and last boot time within the application. This transforms DDI Central from an IP address management tool to an intelligent network visibility platform.

Contextual DHCP lease management

Network admins get to know what kind of devices gained a DHCP lease from the server, with details like OS, hardware details, and MAC address. This helps in learning which IP address is active, but what device the IP got leased to, and whether it is secure or not.

Better network troubleshooting

When reports come in regarding DNS or DHCP issues, admins can correlate the lease usage with the device details, patches, and vulnerabilities to identify issue causing endpoints. They can also check device status, OS, last boot time, and disk usage to find the network issue.

DNS hygiene and forward-reverse consistency

With the OS and hostname info, network admins can detect missing or outdated DNS records of the devices, and can automatically update the DNS entries and remove unwanted DNS data when devices get replaced or updated.

Strengthen security

These statistics help bridge the gap between IT operations and InfoSec by framing the security posture within an operational context. This shared perspective makes it easier for both teams to collaborate effectively, especially when addressing and resolving endpoint risks.

Visual summary over patches and vulnerabilities

DDI Central collects and lays out patch and vulnerability data of the devices through visual representation for better understanding, all in a single window. This reduces the need for network admins to switch between tools to check patch details and vulnerabilities individually.

Comprehensive endpoint health visibility

Admins can evaluate the patch compliance based on the visual summary of the patch, where it displays the installed and missing patches. Also, the missing patches summary based on severity, across drivers, OS/apps, BIOS, and third-party software, helps prioritize patches and troubleshoot faster.

Prioritized risk awareness

Missing patches summary based on severity helps identify high risk vulnerabilities in the devices connected without the need for going through multiple raw data. This allows network admins to for smarter prioritization of issues within the network for faster resolving.

Actionable security insights

Vulnerabilities based on CVSS score helps admins on understanding the endpoints and differentiate which endpoints are vulnerable to get exposed and exploited. It also highlights whether the vulnerabilities get spread into the older systems or the new updated ones through the CVSS2 (old systems) and CVSS3 (new systems) scores.

Proactive patch management

Exploring the vulnerability list gives admins valuable context such as specific vulnerability names and their CVSS ratings. This allows them to focus and address the most severe threats first. Timely patching becomes more efficient and effective, thus enhancing the network's overall security strength.