Enterprise Security, the Fundamentals & Future Scope

Understand enterprise security & mobilising strategies for full endpoint management.

At-A-Glance

In this white paper, we explain how enterprise networks should be designed, what key aspects should IT engineers take care of and what the hard challenges are in enterprise network design.

Enterprises today are burdened with an explosion of personal & IoT devices in the workplace. These threat vectors have increased attack surfaces. Enterprise requirements & its risk mitigation contingencies need to be understood well before deploying network infrastructures.

For Enterprise, we provide UniNAC, our Network Access Controller solution which helps enterprises overcome these challenges through single console manageability, full endpoint compliance, granular control and rapid response corrective action mechanisms.

Executive Summary

Enterprises of all sizes are rapidly transitioning into using wireless for their connectivity requirements. However, the shift from wired connectivity to wireless connectivity has presented enterprises with security risks arising from threats and vulnerabilities in WiFi. It presents crucial challenges with regards to access control, manageability, operational performance and mainly, protection of the company's digital assets.

While security mechanisms have been evolving as newer technologies emerge, IT & networking in enterprises is yet to completely bind streamlined processes. Adopting effective enterprise security strategies helps enterprise ecosystems increase agility of operations.

Enterprises lack contingencies to deal with network related risks, and the lack of proper guidance & inexperienced IT operations is often the culprit. Now, the development of flexible bring-your-own-device (BYOD) cultures, a rapid IoT proliferation and the changing dynamics of fragmented workplaces have further overwhelmed enterprises. Endpoint compliance & mobility management solutions with risk mitigation techniques help enterprises secure a lot of their wireless networking concerns.

We will look at core concepts & requirements within enterprise security and how a Network Access Controller is the key to secure enterprise networking paradigms for information & device protection.

How We Help, the Core and Developments

UniNAC is our on-premise Network Access Controller for enterprises to gain L7 visibility, manageability and operability of the network and the devices connected to it, all through a single pane of glass. Transparency over the network is important for IT operators to look out for potential risks & analysing real-time network health.

For efficiently running critical business operations, it is imperative to provision a stable and reliable network backbone. In an enterprise, security concerns are assigned highest priority to protect the data stored on devices, or in transit. Enterprises need to deploy networks designed to prevent cyberattacks with swift risk mitigation mechanisms.

Let us take a look at what matters the most in enterprise settings, which primary goals need to be set for enterprise network design, and what we do to help you achieve those goals.

Wireless Security Standards & 802.1x for Enterprise

Security standards revolving around WiFi have developed quite extensively since its inception. From WEP, WPA, WPA2 and now WPA2 Enterprise, engineering teams have worked to create more reliable & secure mechanisms for onboarding users. Deploying hardware elements which support latest wireless security standards are an important part of ensuring enterprise network security.

UniNAC uses a robust security mechanism of an inbuilt RADIUS server using WPA2-Enterprise and 802.1x for authentication and authorisation of devices requesting permission to the network. UniNAC can be configured to use protocols like EAP-TLS, CHAP and EAP-TTLS / PAP for authorising access to devices.

Enterprise Mobility Management

The allowance of personal devices into work environments, and the usage of personal devices for work related subject matters pose several threats to enterprise security. For one, a device granted secure access to internal enterprise networks can be hacked into from an external network, and this path can be used attackers can use the compromised device to gain inside access to the enterprise network's sensitive data & devices. But this is just the tip of the iceberg, BYoD brings with itself rogue devices, malware intrusions, theft of data and many more concerns.

Firstly, enterprises must properly define strict BYoD policies & programs. Post this policy structuring process is complete, enterprises should install NAC solutions which enable full endpoint visibility & compliance abilities.

UniNAC allows enterprises to fingerprint devices & profile them for ensuring compliance with the company's defined policies, regarding version control & adherence to other regulatory frameworks. It can track & monitor device activity throughout the enterprise across all levels, with VLAN segmentation for added control and restrictions.

LDAPs and other active directories help administrators control access of people around all enterprise levels.

The Remote Problem

The recent coronavirus pandemic has forced employees to find a new workplace, at home. This transition is here to stay, at least for some time. Organisations, however, have hit security roadblocks relating to VPN connectivity, secure remote networking and protection of data integrity. It is necessary to create secure communication endpoints for ensuring that the integrity of data is not compromised.

UniNAC comes with an out-of-band branch networking solution which takes care of your enterprise's secure connectivity problems. An inbuilt VPN concentrator and edge gateway abilities creates VPN tunnels for securely pipelining all your data.

Remediation with Wireless Intrusion Prevention Systems

Threat agents might deploy rogue access points or there might be misconfigured devices present in the network. If left unresolved at the time of detection, these threats & vulnerabilities can be exploited for full-blown attacks against network postures. A Wireless Intrusion Prevention System (WIPS) helps you detect and prevent such security incidents. UniNAC comes with a policy enforcement function for greater layer 2 security across the entire network.

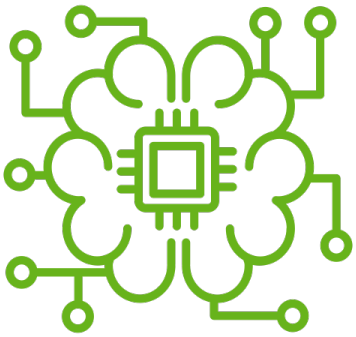
Actionable Network Insights

Enterprise deployments are high availability environments. Data transmission is a continuous process where even the slightest point of failure can disrupt operations & push deliverables ahead of schedule. To ensure seamless operation of these deployments, enterprises must gain real-time actionable network insights for delivering consistent and high performing connectivity without interruptions.

We help with UniNAC's Dashboard, to provide real-time insight with heat-maps, web traffic flow insight and monitoring of critical network infrastructure.

The Role of AI and ML in Enterprise Security

Artificial Intelligence & Machine Learning (ML) models are now being deployed over networks. Gathering insights into the network's health and status through logs and other metrics can help descriptive & predictive ML models to classify, predict and mitigate future threats and faults prior to their occurrences. AI & ML techniques have opened up new paradigms in the networking sphere. Development forecasts suggest that it is highly likely that future networks will be self-managing and self-optimising, with a high level of awareness regarding operations going on over each layer of the network.



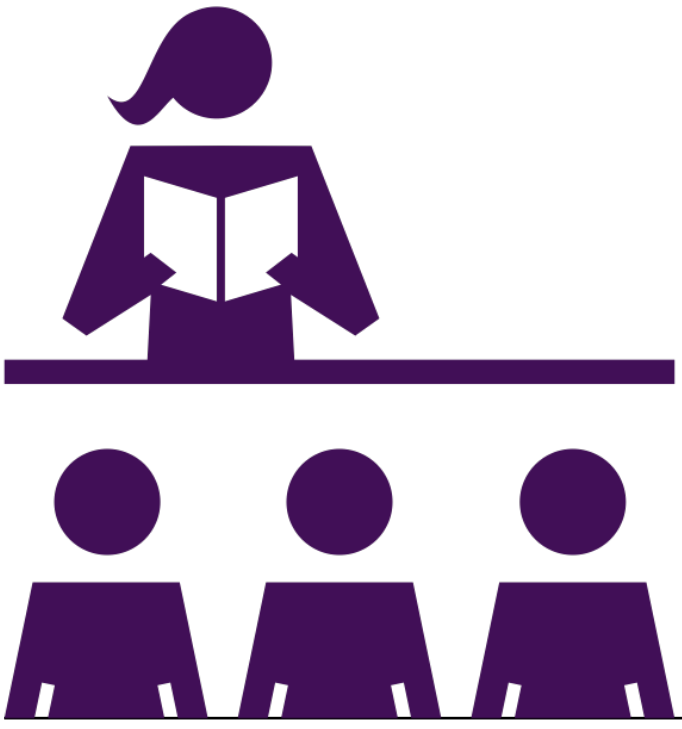
Policy Enforcement & the Principle of Least Privilege

The principle of least privilege implies that, on your network, a user should be granted access only to the degree at which it is necessary. Permission & resource access control based on priority & sensitivity levels is a simple aspect of network security often overlooked.

UniNAC provides policy enforcement mechanisms on a granular level for intrinsic control over the network. Through UniNAC's Dashboard, IT administrators can set policies based on access control, bandwidth, concurrency and group-based routing policies. UniNAC's bandwidth rate limiting policies resolve the issues of bottlenecks. This ensures a seamless experience to all endpoints in your enterprise.

Educating Employees Regarding Security

Compromised IT security is a problem that pervades all business operations, we rely heavily on IT as a business's functional arm. Enterprises should thoroughly educate its employees on the importance of following security protocols, keeping updated softwares and patches for all their devices.



Our Outlook on Next Generation Networking

We believe that the future of enterprise security will be driven by intelligent cloud based analytics from hardware controllers & access points on premise. As enterprises would want to decentralise their workplace data, they would take an approach of locally containerising their cloud facilities and network controls. Software defined networking has already made significant inroads into the networking space. Going ahead, Artificial Intelligence and Machine Learning would lead network insights and optimisation of its resources. The faster enterprises learn and adopt next generation technologies for managing their networks, the quicker they improve their overall efficiency.

About Indio Networks

We are business leaders in the field of wireless networking solutions, and now we are deep diving into IoT & fields related. We bring over 25 years of experience to the table with value innovation, reinvented engineering & high performing solutions.