Next generation cloud security

According to Gartner, 99% of the vulnerabilities exploited by the end of 2020 were the ones known by security and IT professionals at the time of the incident. In fact, one in three breaches are caused by unpatched vulnerabilities.

Software vendors are constantly publishing new patches to fix problems in software that they have sold. It is then up to the users of the software to apply the patches -- or else risk leaving themselves open to attack via the backdoors that the vendors failed to spot when building the product in the first place.

Patch management has historically been a nightmare for IT and security teams: 12,174 common vulnerabilities and exposures (CVEs) were reported last year. The need to test those patches to ensure that they don't cause other unexpected problems, means that there is often a delay in getting systems secured. That leaves a gap that hackers can exploit. According to a new report from IBM and the Ponemon Institute, the average cost of a data breach in 2020 is $3.86 million.

Vulnerabilities - the root cause of most information security breaches

All software has technical vulnerability that crooks can exploit in countless ways. This is why the organisations that maintain those programs routinely look for and address exploits before they are discovered by criminals.

Any time a vulnerability is fixed, the software provider releases a patch, which needs to be applied by the organisations that use the program. This must be done promptly, because crooks – now alerted to the vulnerability – will be actively looking for organisations that are still exposed to the threat.

Nearly 60% of data breaches in the past two years can be traced back to a missing operating system patch or application patch, researchers report. Poor patch management can be linked to the high costs of downtime and disruption. Both of these resulting factors are magnified in larger organizations and are poised to escalate as businesses rush to support fully remote staff as the COVID-19 pandemic continues.

Getting a handle on patch management is an unending challenge for IT and security teams. It takes the average organization 38 days to patch a vulnerability. Even then, 25% of software vulnerabilities remain unpatched for more than a year. Improved patching processes could strengthen enterprise defense against cybercrime but costly downtime and disruptions mean even "fire drill" vulnerabilities don't get patched. One of the biggest obstacles to frequent patching is that security teams struggle to identify

everything that needs to be fixed. Understaffed and struggling with alert fatigue, it can be hard to identify the systems that are yet to be updated, to prioritize remediation, and to apply patches quickly.

It is a scale and prioritization issue. Organizations thinking about vulnerabilities coming at them have to focus on which vulnerabilities to patch and when, rather than ''if'' they are going to reach them.

Securing remote access

Threats and hacking methodologies evolve at an alarming rate, so maintaining awareness and a security-focused mindset is the key to staying secure. Layering multiple solutions for business security is one of the best ways to keep business safe against cyber attacks. Among others, here are some of the solutions that are key to securing an organization's data from vulnerabilities:

- Implementing firewalls (including web application firewalls)
- Administering multi-factor authentication
- Ensuring connections are secure and passwords are strong
- Utilising intrusion detection systems
- Constantly monitoring and updating web platforms

Additional to these measures, cloud based VPNs can also help encrypt data to add an extra layer to your cybersecurity strategy.

One of the most effective protections an organization can implement is a strong network segmentation. Remote users should be limited to only access the systems that are required to perform their job functions. Restrictions should be in place to segment your network to prevent unlimited network access for remote users. Segmenting VPN connections to access only the required systems is paramount in creating a strong security barrier.

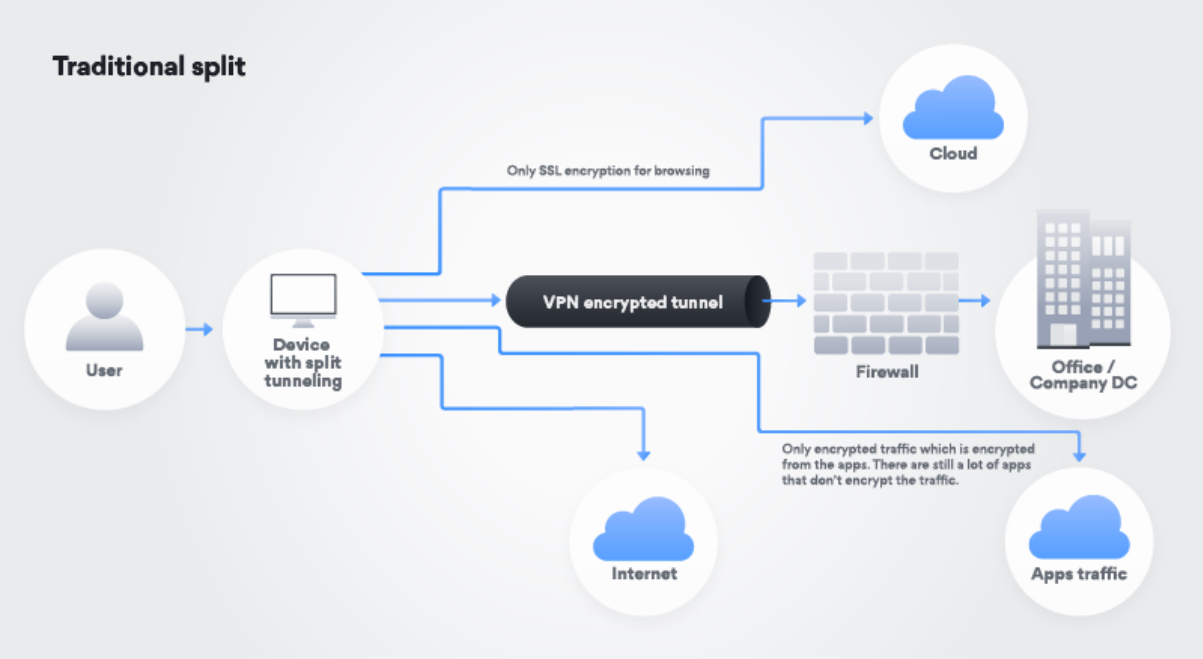
Organizations can also minimize unauthorized access with a fixed IP method. This way they could reduce the risk of IP sharing when a number of devices use the same IP address. Companies therefore have a greater chance to protect themselves from vulnerabilities by changing their firewalls to only allowing certain IP addresses on their whitelist. Hence, hiding the firewalls from the public.

Split tunneling vs NordLayer gateway

With increased traffic due to remote work and with a need to relocate to remote settings quickly, many companies have had to sacrifice security over speed and performance — elevating traffic using split tunneling. Using a business Virtual Private Network (VPN) for remote access involves what and how much data to send down the tunnel. When creating a VPN, network engineers have an option to enable "split-tunneling" which sets a determination of what data traverses the VPN.

Enabling split-tunneling reduces traffic on corporate networks, increases speed through reduced latency for specific tasks, and grants privacy to end users. These key

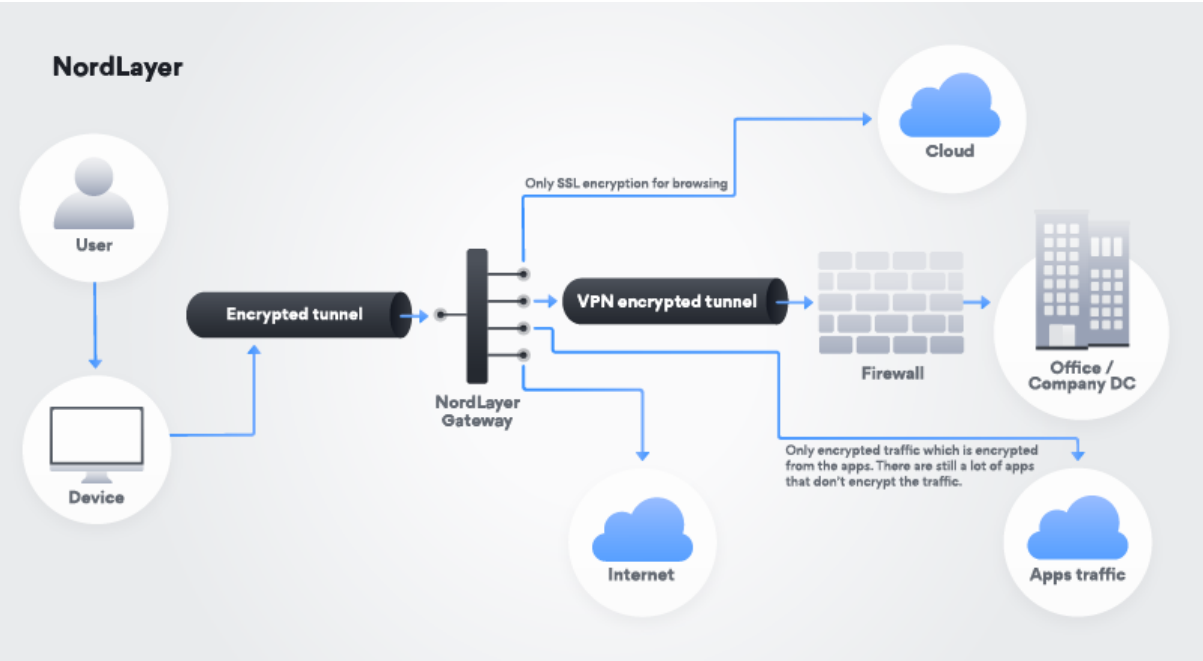
capabilities primarily reduce traffic on internal networks, with most organizations switching to split tunneling when they set up their VPNs. Users that understand this technology appreciate the privacy and enhanced performance through improved routing paths.



The core goal of providing split-tunneling capabilities is simply to give your employees the ability to perform work functions and internet functions from the internet directly. This connectivity gives your users the fastest capability to do their work using the sources that have the fastest network connectivity. Remember, security is an option if you deploy split tunneling.

As seen in the graphic above, the (remote) ‘’user" connects their laptop to the VPN. Split tunnel method/policy then helps to regulate what and how a user can reach the desired target. In other words, a company sets up subnets that are "inside VPN". All other traffic goes directly from the user to the internet without a VPN. External actors cannot access the corporate network because they do not have the software VPN configured on their laptop, access credentials, or possibly a second-factor token to access the internal network (security in layers like 2FA, certificates, and others.). The user has a tunnel to the corporate network to access any apps or shared drives through the VPN connection while still utilizing the local internet connection of the remote user for access to the web or local resources.

If the corporate remote user's desktop is compromised, the VPN can force disconnect and prevent the attack based upon IPS, bad authentication, host inspection, and others. If the resource is internal and not reachable via the internet, disconnecting from the VPN will prevent the user (and attacker) from accessing the desired source.



At the start of the pandemic companies and their employees have been thrust into a remote working environment rather suddenly, with many organizations' remote networking capabilities still not as shielded as their on-site IT infrastructures. This rapid shift has left many unsecured gaps that malicious actors are looking to exploit for financial gain — or to simply disrupt usual operations. The priority therefore is to secure endpoints and implement stronger authentication protocols for the cloud and other off-premises networks.

By passing the traffic via NordLayer Gateway, users can change settings from ''allow all'' to ''deny all'' and only allow users with a fixed IP address to reach the desired source. This works as an additional security layer which hides a firewall from the internet, narrowing down the area of attack.

Remote employees are falling behind in terms of patching

While most enterprises want to prioritize patching and endpoint hardening, they are inhibited by the pace of digital transformation and modern workforce evolution. Businesses often cite the difficulty in patching systems belonging to mobile employees, remote offices, inefficient patch testing, lack of visibility into endpoints, and insufficient staffing in SecOps and IT operations to successfully do so.

Many businesses have started to fully support remote staff in order to protect them from the impact of COVID-19. The shift is likely to exacerbate existing patch management challenges. Organizations are finding it tricky to manage attack surfaces that aren't hidden behind corporate Wi-Fi Firewalls and many employees don't even have their corporate devices at home currently.

When creating a remote work policy, organizations must consider what they want to do in relation to split-tunneling. Businesses need to understand the architectural decisions that go into implementation considerations and clearly understand the impact of those outcomes. One size does not fit all, and architects and engineers need to understand

business needs before making technical decisions.