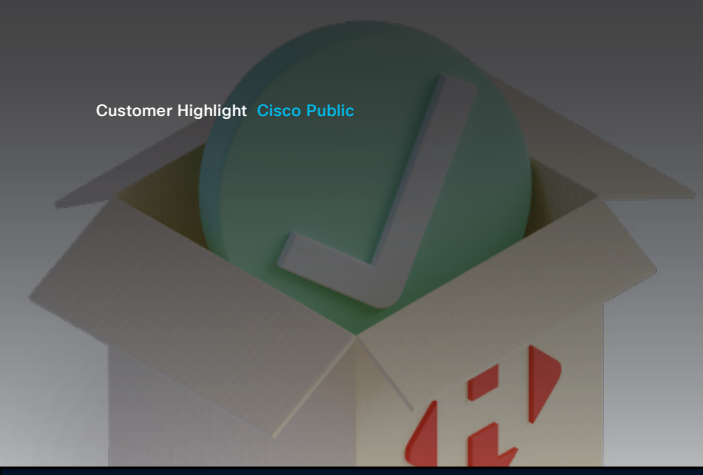

Nova Post Embraces a Universal Approach to Zero Trust with Cisco Secure Access

Industry:
Logistics and Transportation

Location:
Kyiv, Ukraine

Organization:
30,000 employees, 13,837 branches locations across 17 countries

Solution:
Cisco Secure Access

Nova Post, the parent company of the NOVA Group, is a leading logistics and express delivery company headquartered in Ukraine, serving businesses and individuals with a wide range of parcel and freight solutions. Employing 30,000 people, Nova Post operates thousands of branches and parcel lockers nationwide and delivers to 200 countries and regions around the world, including Europe, Canada, China, and the US. NOVA Group also has its own cargo airline company, Supernova Airlines, which manages air cargo and logistics and helps Nova Post provide faster, more reliable international deliveries.

"With Secure Access, we can now assign the right level of access to users or groups through a single, unified console, streamlining an access provisioning process that once took days down to just a few clicks. That means less work for our teams and more time to focus on what really matters."

– Dr. Oleh Polihenko, CISO, Nova Digital

Challenges span critical cybersecurity issues and unique geopolitical complications

Nova Post is a trusted and beloved brand and an essential part of daily life for every Ukrainian, playing a vital role in supporting e-commerce and global connectivity. But operating amid ongoing war, Nova Post faces extraordinary business and security challenges. "On-premises VPNs and other traditional security tools simply can't keep up with the risks we're facing today," says Dr. Oleh Polihenko, CISO at Nova Digital, a dedicated IT company within the NOVA Group. "Between the real threat of physical attacks on our logistics sites and ongoing cyber threats, it's more important than ever that we prioritize business continuity and making our operations highly resilient as we intensely focus on tightening security."

With a growing workforce, expanding network of branches, and a diverse ecosystem of vendors, contractors, and external partners, Nova Post must provide secure access to internal web resources for a wide variety of users, many working remotely or on unmanaged devices. But balancing strong security controls with a seamless user experience proved to be a challenge.

- **Complex Security Infrastructure Hindered Policy Enforcement:** Nova Post was using numerous disparate security tools, including zero trust, VPN, and web traffic filtering solutions, making it difficult for IT to apply and enforce security policies at a granular level.
- **Unsecured Devices Increased Risk:** Providing secure access to internal applications required distributing VPN certificates to personal and BYOD devices, which exposed the organization to risks from potentially unsecured endpoints and increased the complexity of IT management.
- **Traditional VPN Left Network Vulnerable:** Legacy VPN infrastructures are often targeted by cyberattacks exploiting known vulnerabilities, compromised credentials, or misconfigurations, which heightened the risk of unauthorized activity and lateral movement.
- **Disrupted User Experience Impacted Efficiency:** Users experienced inconvenience with security processes, which at times involved repetitive steps like handling VPN certificates when accessing applications and resources.

A Solution that Redefines Secure Access for the Modern Era

As Nova Post looked for a better way to secure access across the organization, they focused on four key goals:

- Strengthening security
- Resolving issues faster
- Reducing IT complexity
- Making things easier for users

"Cisco Secure Access stood out as the solution that could help us achieve all of these objectives – giving us a single, cloud-managed platform to streamline operations, unify policy management, and simplify the entire remote access experience," explains Danylo Skyba, Security Operations Team Lead, Nova Digital.

With Secure Access, Nova Post is embracing Cisco's Universal Zero Trust Network Access (ZTNA) approach, designed to help organizations secure today's dynamic digital landscape. By consistently implementing least privilege access across the organization, Universal ZTNA helps businesses like Nova Post deliver seamless and secure access from users and devices anywhere to applications and data across a hybrid, multi-cloud world.

Securing Private, Internet, and Web Access

Today, many of Nova Post users are protected by Cisco Secure Access – Secure Private Access (SPA), which reduces the company's reliance on VPNs and vulnerable physical infrastructure while enabling granular, least-privilege access for both employees and internal partners to only the internal web applications, dashboards, or endpoints required for their role. For example, SPA protects executives as they access critical analytics and business portals, as well as project teams and contractors as they access only the resources they need. Having both client-based and clientless connection alternatives for ZTNA provides additional flexibility.

Nova Post users are also protected by Cisco Secure Access – Secure Internet Access (SIA) for added security when accessing the internet and SaaS applications. Nova Post plans to extend SPA and SIA protection to additional users in the future.

Fueling Expansion

Cisco Secure Access's cloud-native architecture gives Nova Post the resilience and scalability needed to expand internationally. "We can now provide secure, policy-enforced access for our distributed teams without routing all traffic back through central European data centers —improving performance and allowing us to support users and customers wherever they are," says Skyba.

Results for Connecting Teams Securely and Powering Business Beyond Borders

Streamlined IT Operations and Faster Access Provisioning

Nova Post has significantly reduced the time and resources required to grant users access to internal resources. A process that once required several teams and days can now be managed by a single department within hours: requests are reviewed for compliance and provisioned directly from a centralized console. “With Secure Access, we can now assign the right level of access to users or groups through a single, unified console, streamlining a process that once took days down to just a few clicks,” explains Polihenko. “That means improved efficiency for users, less work for our teams, and more time to focus on what really matters.”

Enhanced Security and Reduced Risk

Nova Post is enforcing granular, least-privilege access across its environment. Only authorized users are permitted to connect to specific web resources or dashboards, rather than being granted broad network access as with the legacy VPN approach. Skyba says this shift dramatically reduces the risk of unauthorized activity and lateral movement within the network, especially from aggressive web scans, bot and crawler activity, and DDoS attempts. “With Cisco Secure Access, these threats have been effectively eliminated.”

Improved User Experience and Flexibility

End users now enjoy a convenient, streamlined access process that not only improves productivity but also makes it easier for traveling executives, contractors, and staff in remote or international locations to securely access the data and tools they need. Prior to Secure Access, users had to perform VPN-related actions many times throughout the day – start, stop, make selections (such as where/how to connect), handle certificates, and more. With Secure Access, users simply navigate to the desired app and gain access, avoiding repetitive steps, saving time, and improving their productivity.

Efficiency Gains and Cost Savings

“Having Cisco manage the front-line gives our team real confidence and peace of mind,” says Polihenko. “By shifting routine security tasks and much of the day-to-day protection to Secure Access’s cloud-native capabilities, our staff can focus on more strategic projects. It’s a big relief for our leadership, especially as we navigate an increasingly complex threat landscape, knowing that we have trusted experts safeguarding our operations.”

Going forward with a Unified Security Platform for Resilience and Growth

Nova Post’s long-term strategy is to expand Secure Access protection to all employees and branches worldwide. While Secure Access runs in parallel with other security tools, like Cisco Umbrella and Cisco Web Security Appliance (WSA), plans are underway to gradually migrate these solutions to Secure Access SIA.

This will enable IT to consolidate management and policy enforcement within a single, unified console.

Cisco Secure Access has become a critical component of Nova Post’s modern, adaptive security infrastructure, integrating with Cisco Duo and Active Directory. The company is evaluating advanced features, such as integrated DLP (Data Loss Prevention) and Remote Browser Isolation (RBI) and considering integration with Cisco SD-WAN to provide seamless, secure connectivity for branches, particularly in new international markets.

“By bringing our security solutions together with Cisco, we’re not just improving our protection – we’re building the foundation for greater agility, efficiency, and resilience,” says Polihenko. “This unified Zero Trust approach gives us the flexibility and adaptability we need to grow and respond to unpredictable and ever-changing cybersecurity, geopolitical, and market challenges.”