Unior Kovaška Industrija

SNAPSHOT

Slovenian Exporter Ships Out Cyberthreats With End-to-End Preventive Security

Industry
Manufacturing and Tourism

Challenge
Protect highly diverse business units from increasingly sophisticated cyberthreats while enabling reliable access to critical applications and network services.

Answer
Palo Alto Networks Security Operating Platform provides high-performance application- and user-based traffic control with intelligent threat prevention across guest and internal business networks as well as endpoints.

Results

- Strengthens cybersecurity across diverse business units with prevention-based technology.
- Prevents exploits from entering through endpoints with no performance impact on devices.
- Reduces the time needed to identify the source of network issues by 80 percent.
- Accelerates responsiveness to make security changes from weeks to hours.
- Frees up network bandwidth, delaying an expansion and avoiding substantial cost.

Unior Kovaška industrija, a leading Slovenian manufacturer, runs four highly diverse business units. As such, the company relies on a wide range of applications and business services – from industrial control systems to supply chain management, from distribution logistics to point-of-sale and reservation systems. This is in addition to core business applications, such as email, accounting, human resource management and digital communication systems. Underpinning all this is a vast information network connecting processes, employees, suppliers and customers.

With more than 3,800 employees in Unior Group, in addition to clients and vendors accessing network services from all types of devices, Unior faced a daunting challenge to keep its network secure and its users safe from exploits. As the threat landscape changed and evermore sophisticated cyberattacks emerged, its legacy firewalls were simply no longer up to the task. They provided limited visibility and no intrusion prevention – only detection.

Recognizing the growing threats to network security and with an eye to the future, Unior decided to replace its legacy firewalls with a next-generation approach to network security. After an intensive evaluation of vendors, Unior chose Palo Alto Networks® Security Operating Platform.

Today, Unior has deployed PA-3020 next-generation firewalls to protect all segments of its network – internet gateway, DMZ, hotel guest network and core business network – as well as more than 100 virtual LANs within each segment. In addition, Unior takes advantage of WildFire® cloud-delivered malware analysis service and Traps™ advanced endpoint protection, elements of the Security Operating Platform.

Ivan Cizel, Unior's IT manager, comments, "Our decision to go with Palo Alto Networks turned out to be a very good one. Over the years, the threat landscape has been constantly changing, and cybercriminals are getting cleverer all the time. It would be more difficult to defend against the kinds of sophisticated attacks we face today without a next-generation security platform like the one we have from Palo Alto Networks."

He continues, "Before, we only had intrusion detection, which was complex to manage. With detection, you know something is wrong in the network, but then you have to troubleshoot to find the problem and figure out a solution. That's only possible during regular business hours; otherwise, nobody is checking. Palo Alto Networks solved that problem with prevention-minded technologies. Now, we stop cyberthreats before they have a chance to cause a problem."

> "The Palo Alto Networks platform is powerful yet very easy to manage. It protects us well, and we don't need to rely on external providers to manage it. It's really the best integrated platform I've seen."
>
> **Ivan Cizel** | IT Manager | *Unior Kovaška industrija*

By including GlobalProtect™ network security for endpoints as part of a comprehensive security strategy, Unior's IT security team extends the protections of the Palo Alto Networks platform to remote and mobile users. This effectively secures access to business applications even when users are not directly connected to the network or when they're accessing it through personal devices.

"Having GlobalProtect provides us with an added level of comfort, knowing we have consistent security across our diverse enterprise and even for remote users," Cizel remarks.

Using App-ID™ and User-ID™ technologies on the Palo Alto Networks platform, Unior can closely control the applications allowed on its network, as well as the users permitted to access them, by tailoring application- and user-based policies for each network segment.

Along with this granular control, the Palo Alto Networks platform provides Unior's IT team with much-needed network visibility that has helped the company strengthen security and significantly improve network performance. Since implementing the Palo Alto Networks platform, Unior can observe activity on the network and react to potentially compromising activities.

This change meant substantial financial savings for Unior. It also led to higher productivity due to curtailing potentially compromising activity. Overall, the company has reduced the amount of time spent to identify the source of a network issue by more than 70 percent because of improved visibility.

Unior has made substantial changes to its network over the years, deploying new endpoints across its manufacturing and tourism operations. This includes end-user workstations and servers as well as a growing number of IoT devices for industrial automation and hotel guest services.

Protecting these endpoints has always been a priority for Unior, but increasingly sophisticated threats had begun to emerge and pose challenges for legacy antivirus/anti-malware approaches. Cizel notes, "Any solution that fails to detect attacks in almost real time is not acceptable for a business like ours. We need to be ahead of these types of attacks."

To take a proactive stance against all kinds of threats that could affect its devices, Unior implemented Traps from Palo Alto Networks. Traps is currently deployed on multiple servers and hundreds of end-user devices, with plans to scale to even more endpoints and eventually replace Unior's legacy antivirus software.

With WildFire working in tandem with Traps and next-generation firewalls from Palo Alto Networks, all files attempting to enter via the endpoints or the network are analyzed before being allowed through. This prevents malicious exploits from ever gaining a foothold inside the company. In some cases, users inadvertently bring in infected documents on USB drives, but Traps and WildFire block these as well. All this is accomplished with no negative performance impact on endpoint devices.

With Traps, Unior now has a way to prevent security issues rather than respond after the fact. That gives the company more confidence that it is doing everything possible to protect its endpoints.

With Panorama™ network security management, Unior also has a single, integrated portal that allows monitoring and management of network security and endpoint protection. It provides one place where Unior's IT team can review logs and investigate incidents, in addition to automated, template-based policy creation and deployment to ensure consistency across next-generation firewalls and the endpoint protection environment. Unior expects the value of Panorama to grow as the company integrates additional physical and virtual next-generation firewalls into its Security Operating Platform deployment.

Consolidated network security management on the Palo Alto Networks platform has also eliminated the need for third-party management and support, which had previously been necessary for the legacy firewalls in absence of specialized, in-house knowledge. The intuitiveness of the Palo Alto Networks platform allows Unior to handle all administration in-house.

"The Palo Alto Networks platform enables us to be more agile," says Cizel. "Before, it could take weeks to make a change in our security environment. Now, we can make changes ourselves in a few hours and save the service fees. That allows us to be much more responsive to the business as Unior continues to grow and expand."

He concludes, "The Palo Alto Networks platform is powerful yet very easy to manage. It protects us well, and we don't need to rely on external providers to manage it. It's really the best integrated platform I've seen."