Higgins
Better painting management

CASE STUDY

Higgins Coatings uses Zero Trust principles to strengthen secure access for its mobile workforce and expands bandwidth

paloalto NETWORKS

IN BRIEF

Customer

Higgins Coatings

Product and Services

Commercial painting

Industry

Construction

Organization Size

1,000 employees

Country

Australia

Website

https://www.higgins.com.au/

Challenges

Higgins Coatings wanted its predominantly mobile workforce to access applications and company resources anywhere and from any device securely, with full visibility of users' activity.

Requirements

+ Sought network and security delivered from the cloud
+ Wanted a modern secure access service edge (SASE) architecture, avoiding having to route all traffic through the data centre
+ Needed complex Layer 7 deployments to cover all points
+ Use Zero Trust principles to provide scalable, role-based, time-based, and device-based access control
+ Integration with SIEM framework

Solution

They chose Palo Alto Networks Prisma Access, for comprehensive, scalable protection with a consistent work-from-anywhere user experience.

Higgins Coatings (Higgins) is the largest family-owned and operated commercial painting contractor in Australia, with a national footprint. Since most of its fleet of painters access company applications remotely or on the go, the company needed to provide a secure connection to the internet, internal applications, and all cloud applications. This need was further amplified with the onset of the pandemic, as the company's mobile workforce suddenly grew from 80% to 100%. It was imperative to ensure that all users could connect safely and consistently to company resources—from anywhere and from any device—which is the task that the IT infrastructure team undertook.

CHALLENGE

Gain consistent, secure access to all applications for mobile users

With 90% of their service catalogue moving to the cloud, Higgins saw the opportunity to have users access their services more efficiently. The company had limited bandwidth, and with the entire workforce becoming mobile due to COVID-19, the existing infrastructure came under immense strain. "Before we made the switch to Palo Alto Networks Prisma Access, we had users manually enabling their VPN to connect to our data centre, accessing resources there and then egressing the data centre to cloud-based service," reflects Angus Smit, IT security and operations manager at Higgins Coatings. "Needless to say, this was an inefficient design."

Higgins needed a secure remote solution for its mobile workforce that enhanced visibility and control, secured traffic initiated from the data centre to mobile users, provided consistent user experience, and could be managed by a small team.

REQUIREMENTS

Protecting all users and all applications—anywhere

Angus and his team wanted a solution that could provide consistent security and visibility regardless of where the user was. They were also looking at improving user experience considerably. A Proof of Concept (PoC) was initiated with clearly defined success criteria:

- **Cloud-based solution:** Given that a majority of the Higgins' service catalogue was cloud-based, users would need to access the company applications anytime and anywhere.
- **Reduce strain on bandwidth:** The company was experiencing bandwidth issues and needed this to be mitigated; users were ingressing and egressing internet traffic via the data centre, causing a bottleneck. Instead of investing more into the data centre, the call was to explore new technologies—the edge and cloud—to gain the advantage of improved performance.
- **Secure access:** Layer 7 firewalls needed to be deployed to ensure inbound and outbound protection to secure against threats.
- **Role-based access:** Role-based access-control-defining privileges and responsibilities for service management, monitoring, configuration changes, and escalation due to any incident.
- **Time-based access:** Time-based access ensures that users access the internet and social media per company policy while also giving users the flexibility to use their personal devices after office hours, with monitoring.
- **Device-based policy:** The ability to configure different policies depending on the device used to access the internet. For instance, given that the workstation has greater access, the controls are more stringent than a mobile phone with reduced access.
- **Security information and event management (SIEM) integration:** Ability to integrate with the on-premises SIEM to which log forwarding had to be completed to gain insights into traffic and create automated responses based on incidents.

> "Before we went down the Palo Alto Networks Prisma Access route, we had users manually enabling their VPN to connect to our data centre, accessing resources there, and then egressing the data centre to cloud-based services. Needless to say, this was an inefficient design."
>
> **— Angus Smit, IT Security and Operations Manager, Higgins Coatings**

SOLUTION

Comprehensive threat intelligence, superior technology and secure access

Higgins and Palo Alto Networks have worked well together for the past five years. Palo Alto Networks solutions are considered best-of-breed, being consistently selected as market-leading by Gartner®. Higgins turned to Palo Alto Networks to implement a strategic Zero Trust initiative to eliminate the concept of trust from their network architecture for both users and infrastructure. Prisma® Access consolidates more point products into a single, converged, cloud-delivered platform than any competing solution, transforming network security and allowing organisations to enable secure hybrid workforces. This meant that Higgins could have their remote users access the internet from the edge or through a cloud provider rather than coming in via their data centre, thereby mitigating the risk of limited bandwidth. Smit goes on to add, "From the get-go, the experience has been seamless. Users are way more satisfied with the internet connectivity, and from an IT point of view, we are happier because users are logging in via always-on, native VPN, with the ability for machines to connect to the service in a pre-logon state."

> "Without a doubt, Palo Alto Networks Prisma Access outperformed competition significantly. They were the only ones to meet all our success criteria, and in fact, the only ones with true Layer 7 protection. The team demonstrated unstinting support during the Proof of Concept. In addition, the metrics derived from the Proof of Concept phase on internet traffic and the insight we got from their logs [were] far superior, culminating in our decision to go with Prisma Access."
>
> **— Angus Smit, IT Security and Operations Manager, Higgins Coatings**

BENEFITS

Zero Trust architecture

With a predominantly remote workforce and cloud transformation, Higgins needed to ensure that their security was keeping pace with their business needs. With Prisma Access, the company can apply Zero Trust principles—eliminating implicit trust—to all their users and across their entire infrastructure. Through the verification of identity, device, and workload, as well as securing the access via role, time, and device, Smit and team have a robust foundation that paves the way for a true Zero Trust enterprise.

Enhanced protection for all app traffic

With user-based, always-on, pre-logon connections, Higgins has now gained insight into what applications are actually being used by end users. Now, all traffic going in and out of workstations has been covered, and the company can monitor what people are installing, whether services accessed are sanctioned and what they are communicating. From a data exfiltration point of view, the company has better insight into a user's behaviour as it is integrated with SIEM, initiating alerts in case certain metrics deviate from the norm. Additionally, the company can now elevate monitoring for specific users, should the need arise.

Unlimited bandwidth for the data centre and improved user experience

Before deploying Prisma Access, Higgins had limited bandwidth within their data centre to cater to their mobile workforce. With Prisma Access, this is no longer an issue. Positive feedback from users indicates that the workforce is far happier now, as the internet is not slow, and cloud-based services face no performance issues. Earlier, given that most of the workforce was mobile, workarounds were paper-based. This has changed now, and the workforce is more productive.

Increased organisational agility and cost savings

The new solution has ensured the safety and security of users working from home and the field. Now, the fleet of painters from Higgins only needs to be given a secure mobile connection, and everything else can be monitored by Prisma Access. This is likely to change the definition and required infrastructure of physical offices and can potentially result in significant cost savings for the company in the future.

Securing the foundation for cloud-enabled services

Going forward, Higgins is looking at plugging in further cloud services to the Prisma Access solution. As the company does away with on-premises services, hardware and data centres, they can integrate API plug-ins for either public or private cloud providers.

CONCLUSION

With Palo Alto Networks, security is now an essential part of the business at Higgins—becoming an enabler of remote work instead of inhibiting it. The reputation for the IT department internally has gone up significantly since the rollout of the new solution, a testament to the pre-sales and professional services side of the Palo Alto Networks team. Prisma Access provides consistency in security policy and management and has helped Higgins overcome the challenge of managing several point solutions. Smit signs off on a positive note, saying, "Our relationship with Palo Alto Networks has only grown stronger with the Prisma Access deployment as the team has constantly demonstrated value and worked with us to resolve our business challenges. We have no doubt that Palo Alto Networks will continue to be a long-term partner for us, and can count on them to deliver suitable solutions as our business requirements change."

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com