

## Remote Work Puts Your Business at Risk

The move to remote work and increasing use of insecure public cloud apps have been a goldmine for cybercriminals who easily steal login credentials to gain access to your critical data.

So, how do you enable collaborative work from anywhere without putting your business at risk?

## Introducing Overwatch SaaS Security

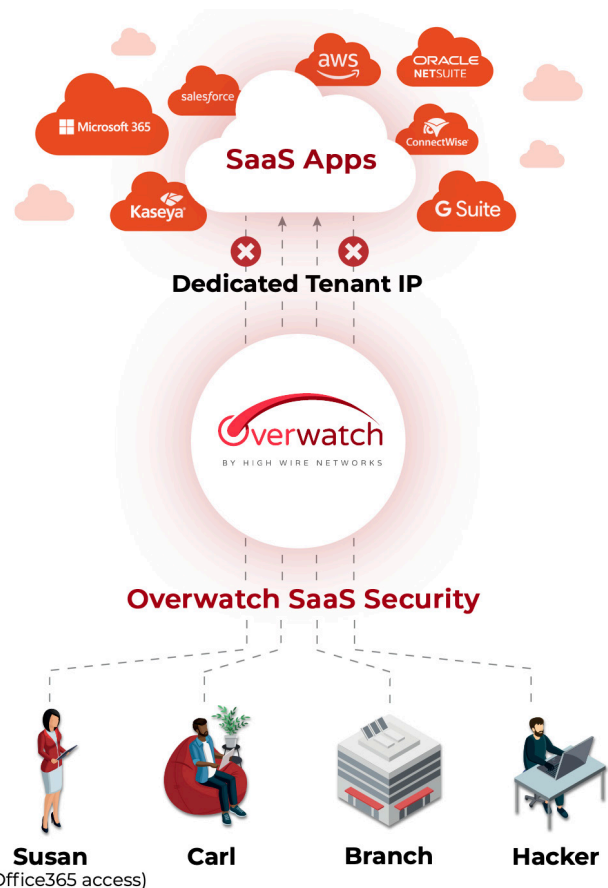
With Overwatch SaaS Security powered by ZTEdge, you can lock down vital software-as-a-service (SaaS) applications while supporting unlimited collaboration with your remote teams.

### Overwatch SaaS Security:

- Prevents the use of stolen user credential to access SaaS apps from the public Internet.
- Restricts access to cloud apps only to users logging in via the zero-trust network.
- Blocks employees from using risky cloud applications
- Sanitizes downloads to protect devices from weaponized files
- Limits the ability of users share data on cloud apps

**Plus, your SaaS security is managed round the clock from the Overwatch Security Operations Center, giving you the added protection, including:**

- 24/7 monitoring by expert analysts
- Real-time threat detection and response
- Continuous policy management



### Expert Protection Delivered as a Service

You don't have to be a security expert to deploy Overwatch SaaS Security. We're making it available to businesses of all sizes as a managed service.

**✔ Affordable Subscription**

Get zero-trust access control over your SaaS apps as a cost-effective expertly managed service.

**✔ Easy Deployment**

Give employees zero-trust access to their SaaS apps by downloading agents on all internet-enabled user devices.

**✔ Fully Managed**

We configure, monitor and respond to threats from our 24/7 Security Operations Center (SOC).

### Benefits of Overwatch SaaS Security

Overwatch SaaS Security delivers unprecedented control over access to critical cloud apps, including the following benefits.

**✔ Credential & App Protection**

Our secure access service edge (SASE) framework prevents access to apps and user credentials from the public internet.

**✔ Unique, Portable IP Addresses**

Unique, personal IP addresses assigned by the Cloud Access Security Broker prevent lateral attacks vectors.

**✔ Policy Enforcement**

Continuous monitoring enforces user, group, location and/or device-based policies for SaaS applications.

**✔ 24/7 Monitoring**

Always-on monitoring by our industry-leading SOC analysts enables real-time managed detection and response to threats.

### Cybersecurity, Simplified

Overwatch SaaS Security is part of High Wire Networks' Overwatch Open Prevention Suite (OPS). Combined with a managed detection and response platform, Overwatch offers organizations end-to-end protection for networks, data, endpoints and users. With one affordable subscription and a security appliance at every location, you can take advantage of these key features:

- ✔ Security Operations-as-a-Service with Open-XDR**
- ✔ Real-time Patch Management**
- ✔ Managed Network Detection and Response**
- ✔ Multi-factor Authentication**
- ✔ Security Awareness Training**
- ✔ Video Surveillance-as-a-Service**
- ✔ Zero Trust Remote Access**
- ✔ Continuous Vulnerability Assessments**
- ✔ Managed Firewall**

Overwatch also delivers the critical benefits your organization needs:

<b>✔ Integrated, Best-of-breed Solutions</b>	<b>✔ Scalable &amp; Future-proof Architecture</b>	<b>✔ 24/7 Protection &amp; Response</b>	<b>✔ Data Sovereignty</b>
<b>✔ Threat Detection, Blocking &amp; Elimination</b>	<b>✔ Continuous Compliance</b>	<b>✔ On-demand Reports &amp; Dashboards</b>	<b>✔ Predictable Costs &amp; No Capital Outlay</b>