

Ransomware on the Rise

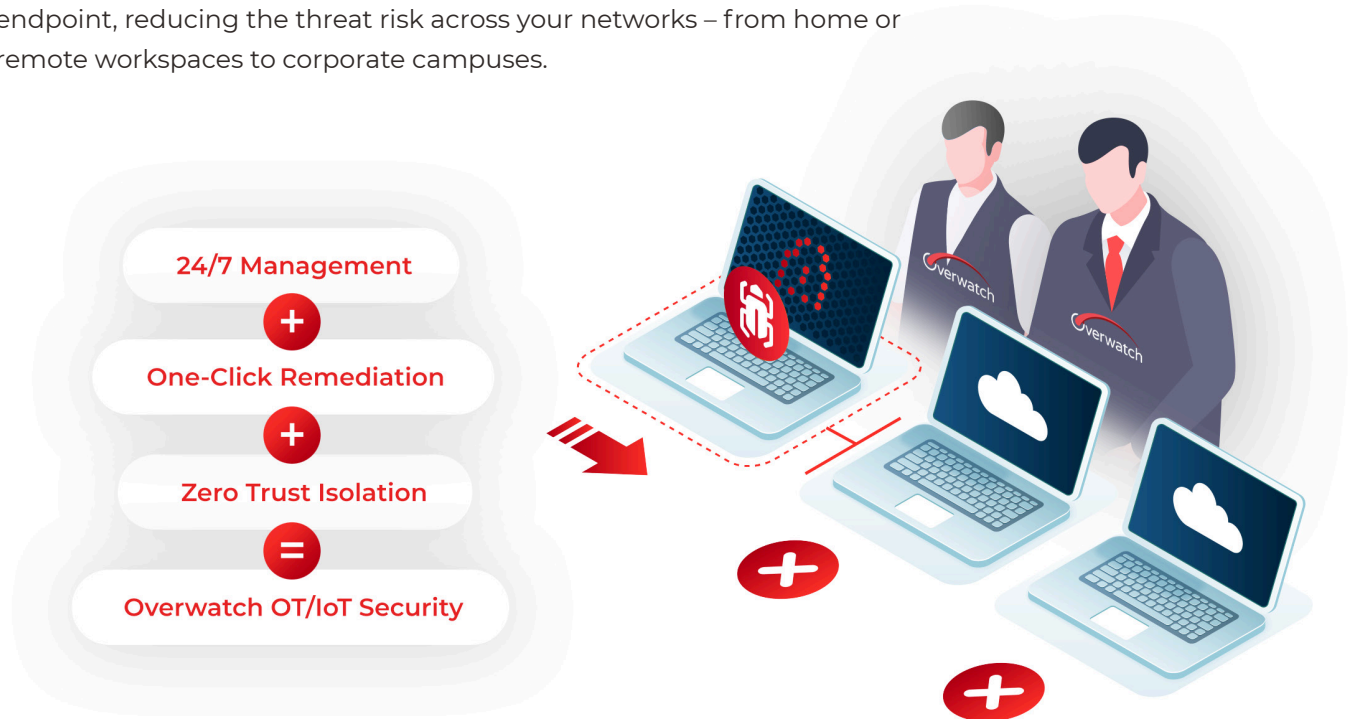
Cybercriminals are getting rich by literally holding corporate data and networks hostage. Ransomware attacks are on the rise because they work. They're hard to detect and almost impossible to stop – until now.

Introducing Overwatch OT/IoT Security

With one click, Overwatch 24/7 security analysts can lock down your business network, isolating the threat so it can't move between devices or locations, minimizing potential impact and damage. And it's made possible without any agents or changes to your network infrastructure.


Stop Ransomware in its Tracks

Overwatch OT/IoT Security blocks all unnecessary network communications to or from any endpoint, reducing the threat risk across your networks – from home or remote workspaces to corporate campuses.




Expert Protection Delivered as a Service

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


 **Affordable Subscription**
Get unprecedented zero-trust isolation as a cost-effective expertly managed service.


 **Easy Deployment**
Deploy with ease. No agents, APIs, design changes or forklift upgrades.


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


Benefits of Overwatch OT/IoT Security


Overwatch OT/IoT Security delivers the industry's most potent ransomware defense solution, including the following benefits.

 **Zero Trust Approach**
Protect IoT devices by starting from a place of least privilege - thereby reducing the attack surface.

 **Instant Mitigation**
Reduce the "blast radius" of any attack to a single endpoint by halting communication between workstations and applications.

 **Pre-incident Preparation**
Using network access and protocol control policies, set response by attack severity to stop ransomware spread at the source.

 **Automation & Integration**
Programmable API interfaces enable our Open XDR security solution to boost ransomware remediation at remote endpoints.

 **Quick Recovery**
Once the ransomware attack is fully eliminated, one-click remediation can be used in reverse to instantly normalize the network.

Use Cases in Healthcare and Manufacturing

With the rise in critical device IoT implementation in medical spaces or manufacturing, comes the added complexities of securing internet connected devices that can't benefit from additive software protections, such as EDR. To address these concerns, agent-less solutions like Overwatch OT/IoT Security are required to segment the IoT devices from the general local area network.

Two primary benefits for microsegmentation:

1 Limiting the attack surface for individual devices; hence limiting the scope of malicious activity/ransomware in the environment by preventing devices from having general access to the network

2 Providing increased logging potential from such devices that otherwise would be not primed to share such telemetry with a security monitoring service