OPSHIELD

Protection Pack Datasheet

Challenge: Threats evolve

Each month, researchers at ICS CERT, Wurldtech, and other organizations discover new cyber threats and vulnerabilities in operational technology (OT).

And each month, inadvertent and malicious incidents use old OT vulnerabilities that haven't been patched or protected.

Don't run critical operations without up-to-date protection for your OpShield deployment.

Solution: Regular updates

Protection Packs are the updates your critical infrastructure environment needs to keep pace with today's changing risk landscape.

OpShield Protection Packs feature, on average, 90% high or medium severity protections. We help protect vulnerabilities against current and future threats that are most dangerous to your operations.

wurldtech
A GE Company

OpShield Protection Packs
Threats evolve–so can you

In the past year, 67% of companies with critical infrastructure suffered at least one attack. In the next year, 78% expect to be successfully compromised.[1]

Deploying OpShield provides a strong foundation against such attacks. The next step is keeping your protection updated as new threats emerge and existing threats evolve.

OpShield Protection Packs are continual–at least monthly–signature updates that allow OpShield to protect against threats that exploit control system vulnerabilities.

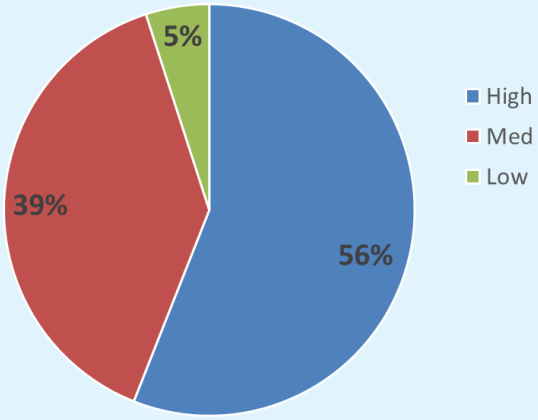
Your subscription funds an industry-leading research team focused exclusively on OT cyber security. We are vulnerability-driven, so rather than chasing hundreds of threats for each control system vulnerability, we research what the threats are exploiting and create a vulnerability signature to protect against current and future exploits.

[1]Unisys and Ponemon, 2014

Benefits

- **Visibility:** Identify intrusions into your network by attackers exploiting known vulnerabilities.
- **Lasting protection:** You can address vulnerabilities, not just exploits. Protection Packs address the root cause of vulnerabilities, providing the highest level of protection until a patch can be installed.
- **Critical focus:** Stay up to date on the most critical threats that could cause unplanned downtime and operational havoc. The average CVSS Score of detected issues is >7.0 (High Severity).

Released Protections by CVSS



NEXT STEPS

For more information or a product trial, please contact Wurldtech sales:
Toll free: 1 877 369 6674
Email: sales@wurldtech.com
or visit **wurldtech.com**

What's in an OpShield Protection Pack?

Each Pack contains signatures for 10 to 20 of the latest vulnerabilities facing critical infrastructure operators. We focus on high-impact vulnerabilities, with 95% of our protections addressing high- or medium-severity vulnerabilities.

The team issues OpShield Protection Packs at least monthly to keep you up to date with the latest operational technology cyber security threats and vulnerabilities.

To use a Protection Pack subscription, you must have OpShield securing your environment.

Sample monthly update summary

OPSHIELD

Vulnerability Signature Update

March 2016 - Document WST-014-0003

For Versions 1.6.0+	OpShieldSignature_0041-R1.7-2016-03.asg MD5 1001994B3D5FE94A53563219FD4E358A SHA-1 26504CBCE816626629EC6046453C5423C84A7C04

To update your OpShield signatures:

1. Log into the OpShield management console.
2. Navigate to the **Policy** page. Click the **Signature** tab.
3. Click the **Import** button to open the **Import Signature File (.asg)** dialog.
4. There are two ways to import signatures into the database:
5. Click Select files to browse for and select the file.
6. Drag and drop a file into the drop files here to upload area.

Once you have selected the Vulnerability Signature Update file, the **Import Signature Files** dialog will close and the OpShield will import the signatures into its database.

This OpShield Vulnerability Signature Update contains ##### new signatures for products such as PLACEHOLDER PLACEHOLDER PLACEHOLDER PLACEHOLDER PLACEHOLDER PLACEHOLDER. It also contains ###### updated signatures for PLACEHOLDER PLACEHOLDER PLACEHOLDER PLACEHOLDER.

New Signatures

ID	Signature Name	CVSS 2.0 Score
758	InduSoft Web Studio Remote Code Execution	9.3
934	Yokogawa CENTUM BKBCopyD.exe Stack Based Buffer Overflow	8.3
1012	Advantech WebAccess Dashboard Authentication Bypass	10.0
1013	SearchBlox Config File Exfiltration	6.4
1014	GE D20 Data Concentrator TFTP Server Multiple Vulnerabilities	9.4
1015	GE Proficy Real-Time Information Portal Directory Traversal	6.4
1016	Unitronics VisiLogic OPLC IDE TeeChart.ChartGrid ChartLink/ColWidth ActiveX Remote Code Execution	6.8
1017	Unitronics VisiLogic OPLC IDE TeeChart.ChartGridNavigator.5 ActiveX Control GridLink Remote Code Execution	6.8
1018	Unitronics VisiLogic OPLC IDE TeePreviewer.ITeePreviewer ActiveX Control ChartLink Remote Code Execution	6.8