OX IT Solutions Ltd

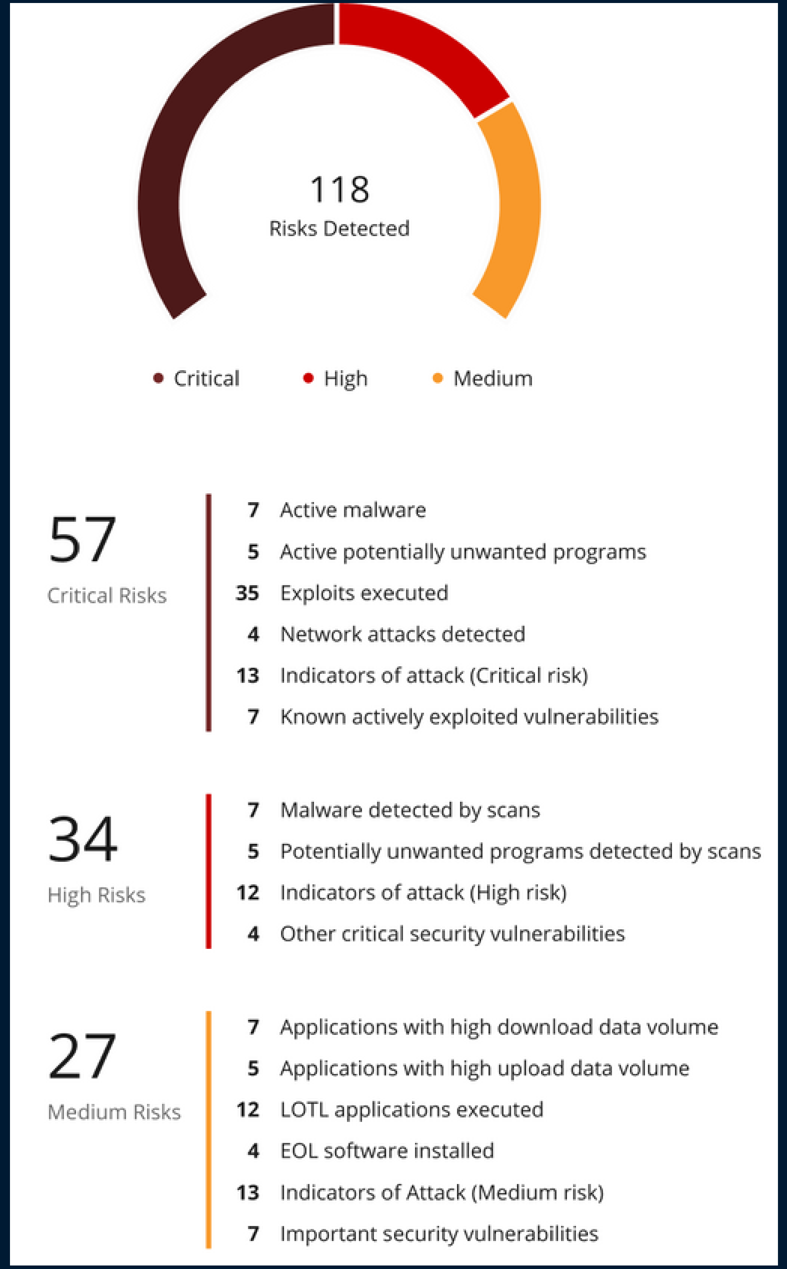
Free & non-intrusive

Endpoint Risk Assessment

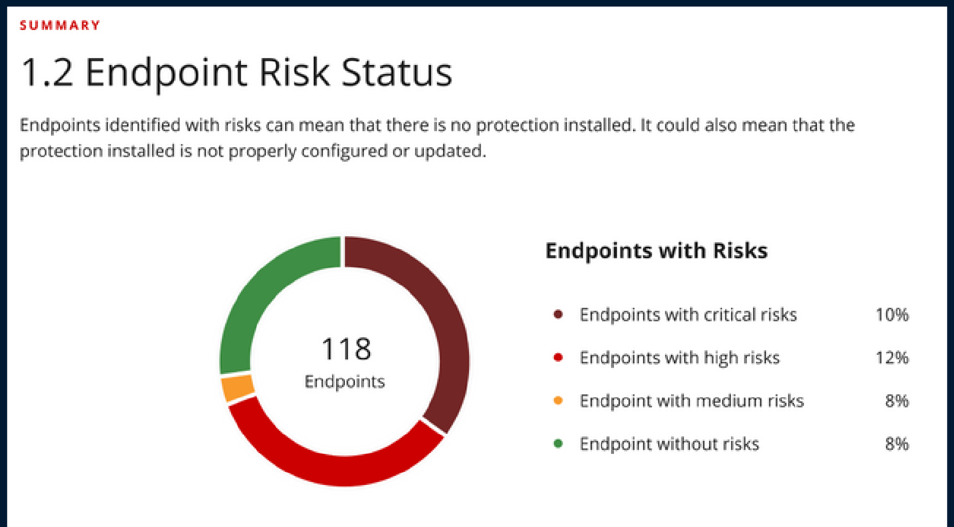
WatchGuard

COMPANY NAME

WatchGuard Endpoint Risk Assessment



57 Critical Risks	7	Active malware
	5	Active potentially unwanted programs
	35	Exploits executed
	4	Network attacks detected
	13	Indicators of attack (Critical risk)
	7	Known actively exploited vulnerabilities
34 High Risks	7	Malware detected by scans
	5	Potentially unwanted programs detected by scans
	12	Indicators of attack (High risk)
	4	Other critical security vulnerabilities
27 Medium Risks	7	Applications with high download data volume
	5	Applications with high upload data volume
	12	LOTL applications executed
	4	EOL software installed
	13	Indicators of Attack (Medium risk)
	7	Important security vulnerabilities

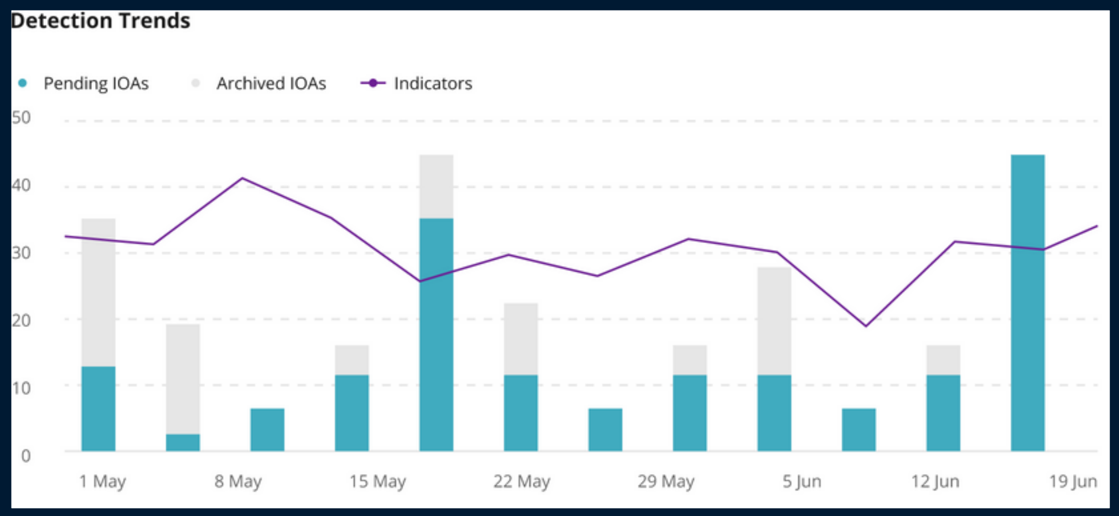

SUMMARY

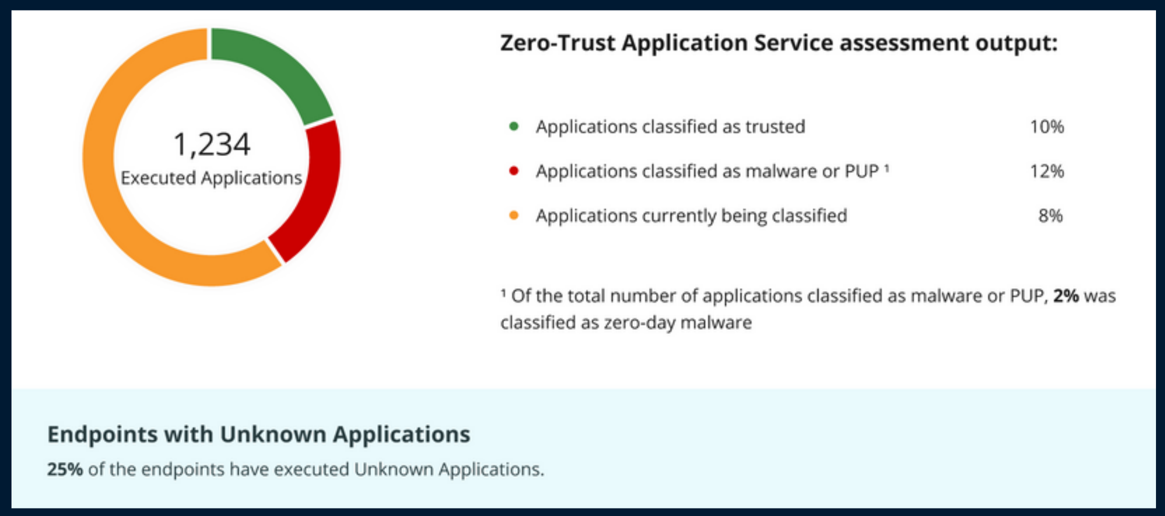
1.2 Endpoint Risk Status

Endpoints identified with risks can mean that there is no protection installed. It could also mean that the protection installed is not properly configured or updated.

Endpoints with Risks

● Endpoints with critical risks	10%
● Endpoints with high risks	12%
● Endpoint with medium risks	8%
● Endpoint without risks	8%


Detection Trends



Zero-Trust Application Service assessment output:

● Applications classified as trusted	10%
● Applications classified as malware or PUP [1]	12%
● Applications currently being classified	8%

[1] Of the total number of applications classified as malware or PUP, **2%** was classified as zero-day malware

Endpoints with Unknown Applications

25% of the endpoints have executed Unknown Applications.

WatchGuard

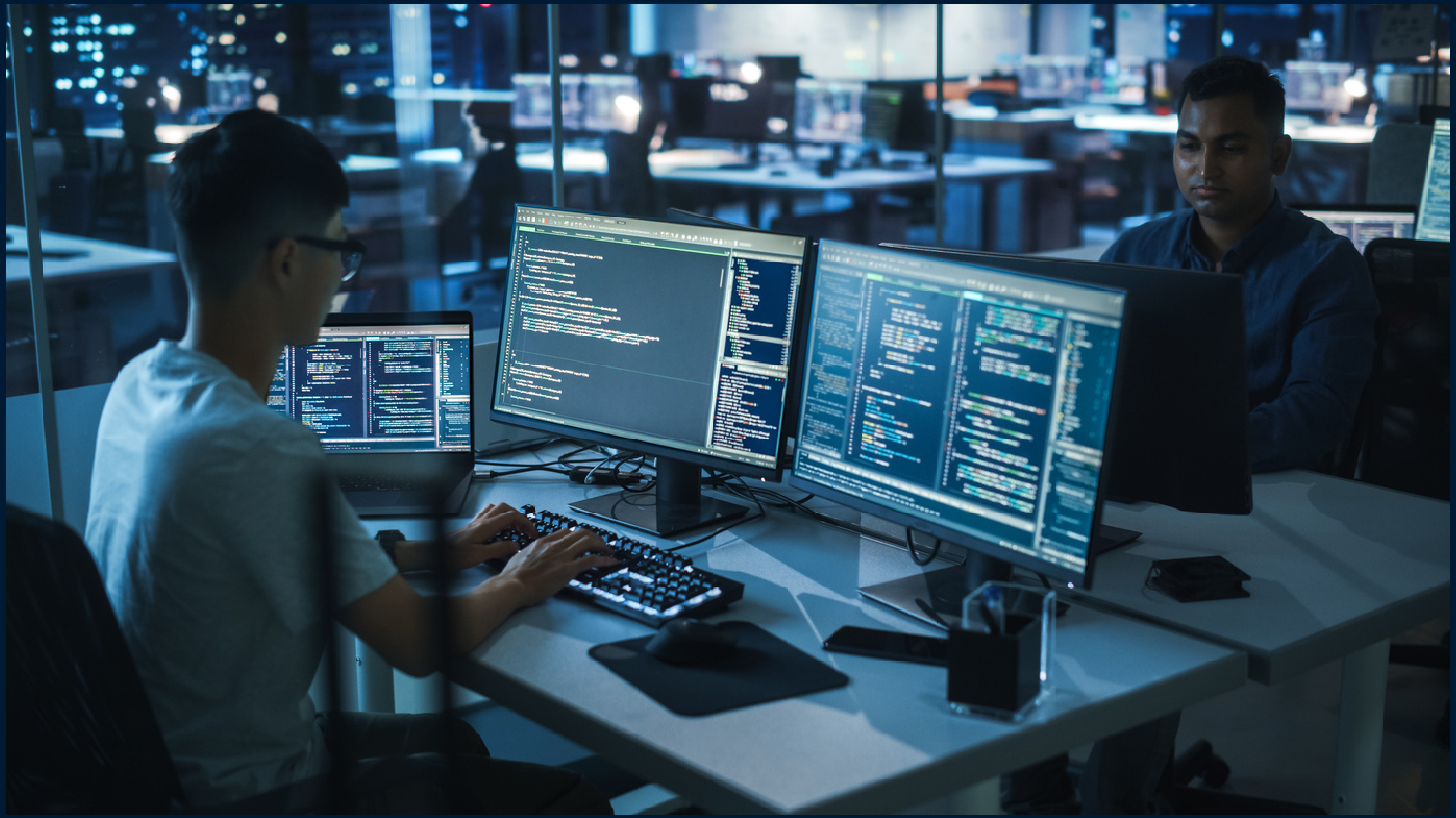
OX IT Solutions Ltd

What is an Endpoint Risk Assessment?

WatchGuard

What is a WatchGuard Endpoint Risk Assessment?

"WatchGuard Endpoint Risk Assessment is a reliable and non-intrusive tool to evaluate the security status of your organisation at no cost!"



WatchGuard

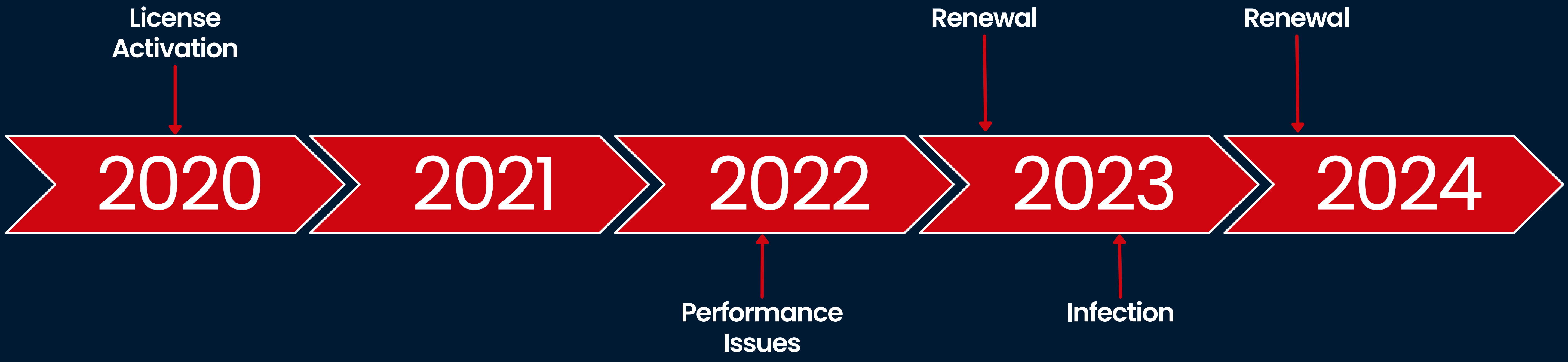
OX IT Solutions Ltd

Why have an Endpoint Risk Assessment?

Why have an Endpoint Risk Assessment?

RIP-AND-REPLACE

A competitor's Endpoint Security solution life cycle



License Activation

Renewal

Renewal

2020

2021

2022

2023

2024

Performance Issues

Infection

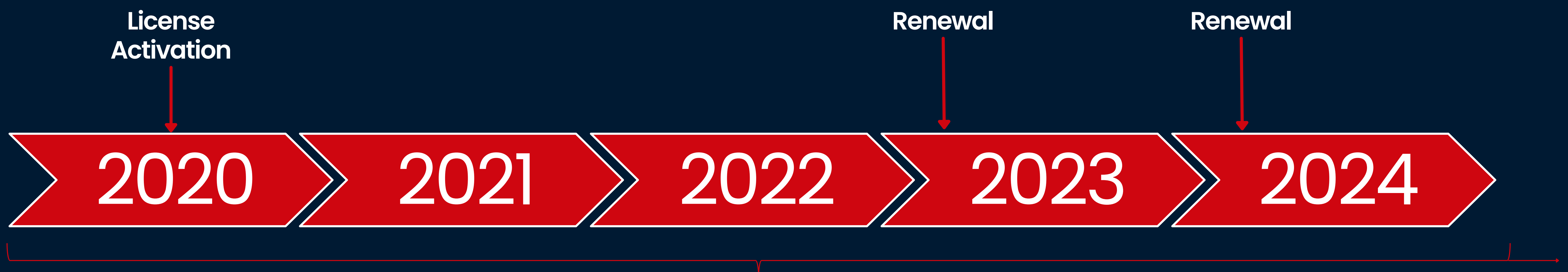
WatchGuard

OX IT Solutions Ltd

Why have an Endpoint Risk Assessment?

A competitor's Endpoint Security solution life cycle

RIP-AND-REPLACE


License Activation

Renewal

Renewal

2020

2021

2022

2023

2024

You should be looking to improve your security posture at all times

Problem

- No proactive measures taken
- Not all solutions provide the same degree of protection

Consequences

- Get infected
- Non-predictable costs
- Negative impact on reputation and customer loyalty

Solution

- **Evaluate & improve security posture with a free WatchGuard Endpoint Risk Assessment**

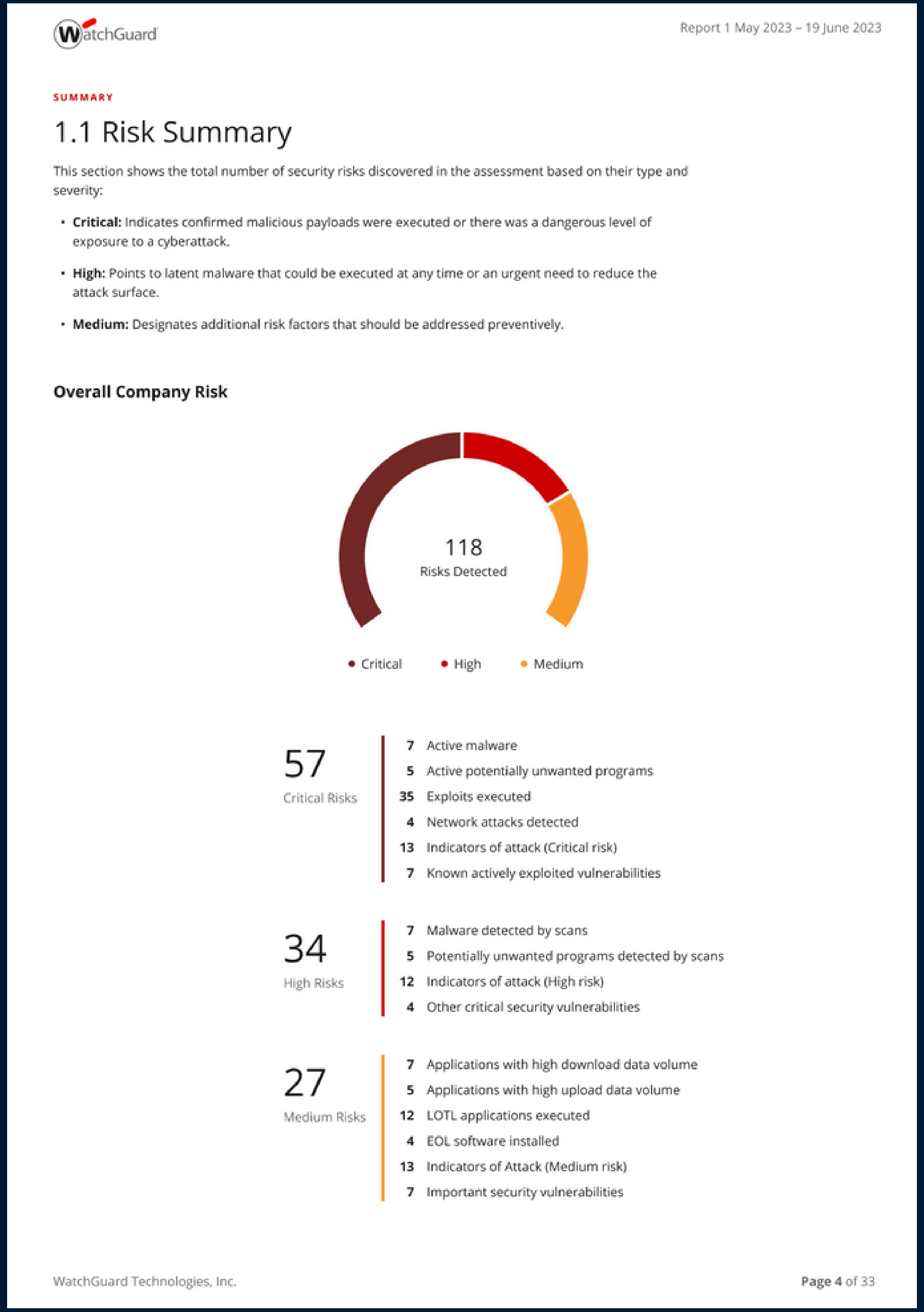
WatchGuard

OX IT Solutions Ltd

Who needs an Endpoint Risk Assessment?

- **Anyone that wants to make sure their security stack is at the right level**
    - We will find higher risks levels in lower grade security environments:
        - Users using “free” Windows Defender or solutions without out-of-the-box EDR services: Webroot, Avast, Malwarebytes, etc.
        - Unpatched operating systems and applications
        - No security awareness for users and/or administrator privileges for all
- **Even with an Advanced EDR solution deployed**, you will benefit from our free Risk Assessment
    - Zero Trust Application Service output
    - Identify actively exploited vulnerabilities present in your endpoints

      EOL software and LOTL applications: Tor or P2P, VPNs, remote connection tools, cloud storage applications and bandwidth consumption



Report 1 May 2023 – 19 June 2023

SUMMARY

1.1 Risk Summary

This section shows the total number of security risks discovered in the assessment based on their type and severity:

- **Critical:** Indicates confirmed malicious payloads were executed or there was a dangerous level of exposure to a cyberattack.
- **High:** Points to latent malware that could be executed at any time or an urgent need to reduce the attack surface.
- **Medium:** Designates additional risk factors that should be addressed preventively.

Overall Company Risk

57 Critical Risks

7	Active malware
5	Active potentially unwanted programs
35	Exploits executed
4	Network attacks detected
13	Indicators of attack (Critical risk)
7	Known actively exploited vulnerabilities

34 High Risks

7	Malware detected by scans
5	Potentially unwanted programs detected by scans
12	Indicators of attack (High risk)
4	Other critical security vulnerabilities

27 Medium Risks

7	Applications with high download data volume
5	Applications with high upload data volume
12	LOTL applications executed
4	EOL software installed
13	Indicators of Attack (Medium risk)
7	Important security vulnerabilities

WatchGuard Technologies, Inc.

Page 4 of 33

So how long does it take?

Assessment Timeframes

- 1-50 seats = **2 weeks**
  - *The deployment should take from minutes to a couple hours max.*
    - *Our Endpoint Security products are fully compatible with third-party AV/EDR products*
  - *Under most circumstances, this should be enough to learn and evaluate running processes and their behaviour*

- 51-250 seats = **3 to 4 weeks**
  - *If there are multiple locations, the period can also be increased to **3-4 weeks***

- 250+ seats: **4 weeks** – but it can be extended up to 60 days
  - *If >250 endpoints are going to be deployed, we'll submit a request for additional licenses*

- Upon completion: **Assessment Review Meeting**
  - *We can engage relevant stakeholders for a Risk Management discussion*
  - *We'll ensure you clearly understands the risks identified and potential implications*
  - *We will then walk you through how the results are obtained and answer any questions you may have*

WatchGuard

OX IT Solutions Ltd

Endpoint Risk Assessment Report

- **Summary**
  - Risks detected classified by type and severity
  - High risk endpoints
  - Zero Trust Application Service
    - 3 of every 1,000 unknown files we classify are new malware!
  - Threat Hunting Service

- **Detailed information**
  - Malware and PUPs
  - Exploits and network attacks
  - Indicators of Attack
  - Vulnerabilities
  - EOL software
  - Programs with high download/upload volume
  - LOTL applications

WatchGuard

COMPANY NAME

WatchGuard Endpoint Risk Assessment

1 May 2023 – 19 June 2023

Duration: 25 days

Number of Endpoints: 34

WatchGuard

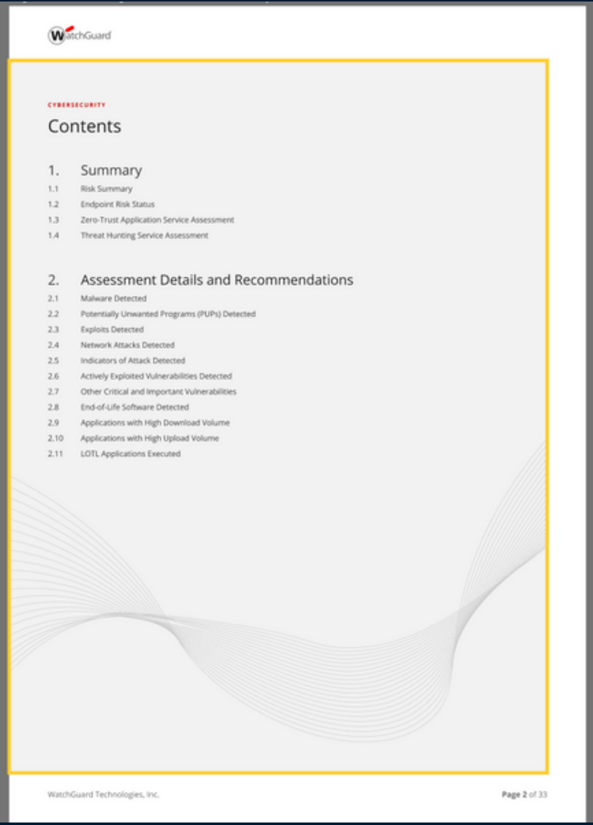
OX IT Solutions Ltd

Endpoint Risk Assessment Report Example

COMPANY NAME

WatchGuard Endpoint Risk Assessment

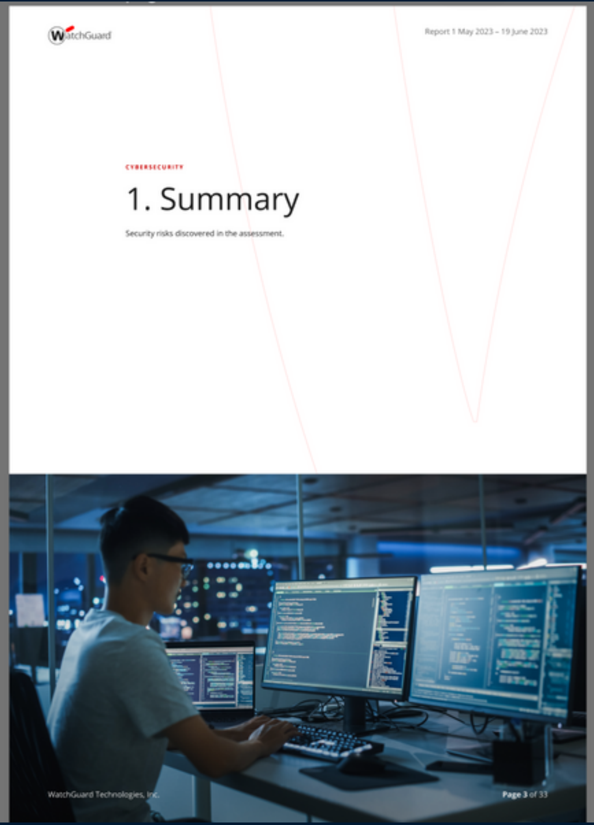
1 May 2023 – 19 June 2023



CYBERSECURITY

Contents

WatchGuard Technologies, Inc. Page 2 of 33



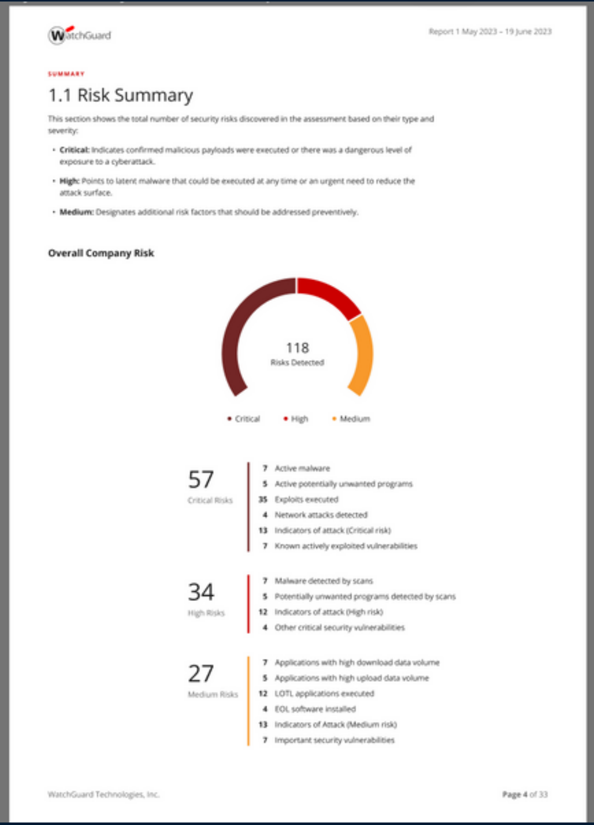
Report 1 May 2023 – 19 June 2023

CYBERSECURITY

1. Summary

Security risks discovered in the assessment.

WatchGuard Technologies, Inc. Page 3 of 33



Report 1 May 2023 – 19 June 2023

SUMMARY

1.1 Risk Summary

This section shows the total number of security risks discovered in the assessment based on their type and severity:

- **Critical:** Indicates confirmed malicious payloads were executed or there was a dangerous level of exposure to a cyberattack.
- **High:** Points to latent malware that could be executed at any time or an urgent need to reduce the attack surface.
- **Medium:** Designates additional risk factors that should be addressed preventively.

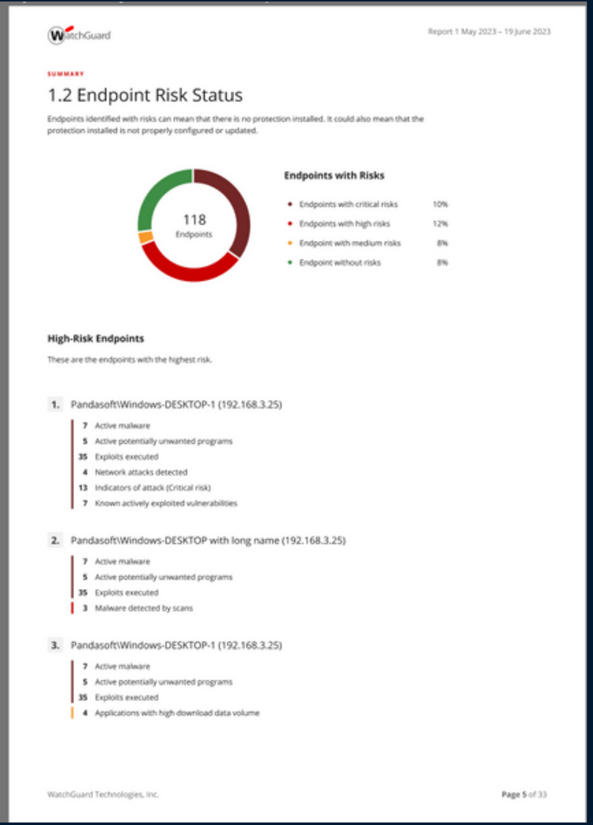
Overall Company Risk

57 Critical Risks
- 7 Active malware
- 5 Active potentially unwanted programs
- 35 Exploits executed
- 4 Network attacks detected
- 13 Indicators of attack (Critical risk)
- 7 Known actively exploited vulnerabilities

34 High Risks
- 7 Malware detected by scans
- 5 Potentially unwanted programs detected by scans
- 12 Indicators of attack (High risk)
- 4 Other critical security vulnerabilities

27 Medium Risks
- 7 Applications with high download data volume
- 5 Applications with high upload data volume
- 12 LOTL applications executed
- 4 EOL software installed
- 13 Indicators of Attack (Medium risk)
- 7 Important security vulnerabilities

WatchGuard Technologies, Inc. Page 4 of 33



Report 1 May 2023 – 19 June 2023

SUMMARY

1.2 Endpoint Risk Status

Endpoints identified with risks can mean that there is no protection installed. It could also mean that the protection installed is not properly configured or updated.

Endpoints with Risks

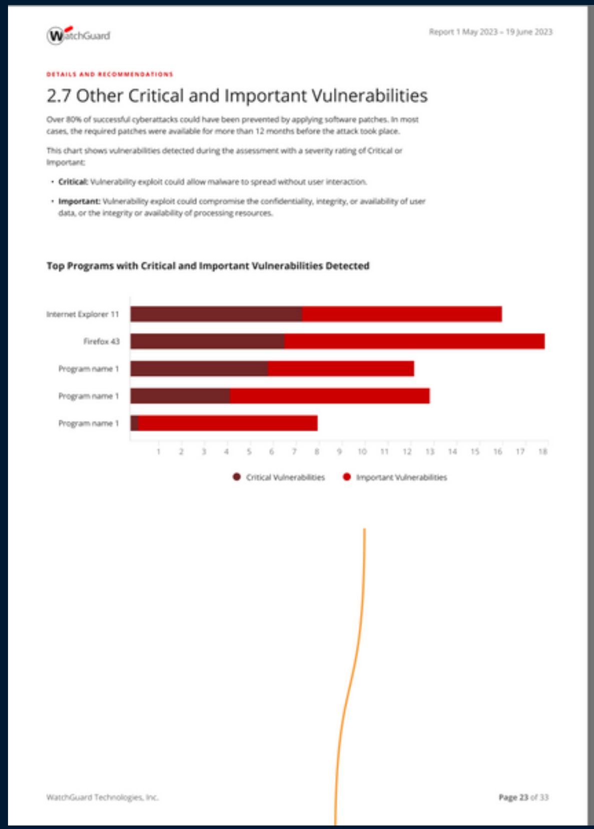
Endpoints with critical risks	10%
Endpoints with high risks	12%
Endpoint with medium risks	8%
Endpoint without risks	8%

High-Risk Endpoints

These are the endpoints with the highest risk.

1. PandasoftWindows-DESKTOP-1 (192.168.3.25)
   - 7 Active malware
   - 5 Active potentially unwanted programs
   - 35 Exploits executed
   - 4 Network attacks detected
   - 13 Indicators of attack (Critical risk)
   - 7 Known actively exploited vulnerabilities
2. PandasoftWindows-DESKTOP with long name (192.168.3.25)
   - 7 Active malware
   - 5 Active potentially unwanted programs
   - 35 Exploits executed
   - 3 Malware detected by scans
3. PandasoftWindows-DESKTOP-1 (192.168.3.25)
   - 7 Active malware
   - 5 Active potentially unwanted programs
   - 35 Exploits executed
   - 4 Applications with high download data volume

WatchGuard Technologies, Inc. Page 5 of 33



Report 1 May 2023 – 19 June 2023

DETAILS AND RECOMMENDATIONS

2.7 Other Critical and Important Vulnerabilities

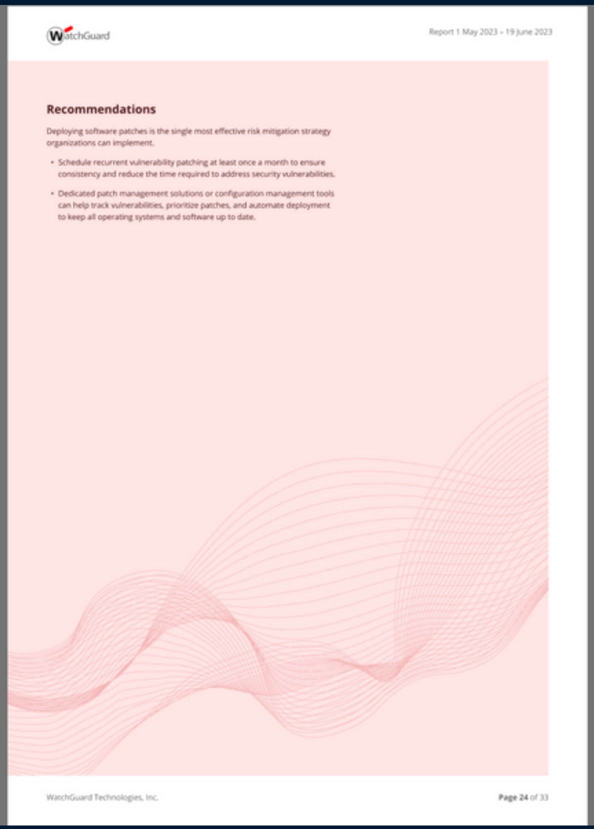
Over 80% of successful cyberattacks could have been prevented by applying software patches. In most cases, the required patches were available for more than 12 months before the attack took place.

This chart shows vulnerabilities detected during the assessment with a severity rating of Critical or Important:

- **Critical:** Vulnerability exploit could allow malware to spread without user interaction.
- **Important:** Vulnerability exploit could compromise the confidentiality, integrity, or availability of user data, or the integrity or availability of processing resources.

Top Programs with Critical and Important Vulnerabilities Detected

WatchGuard Technologies, Inc. Page 23 of 33



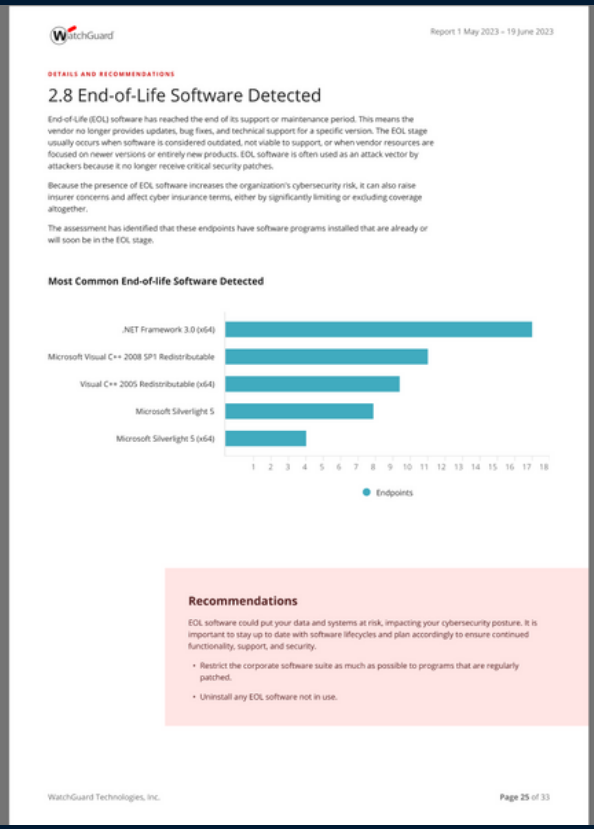
Report 1 May 2023 – 19 June 2023

Recommendations

Deploying software patches is the single most effective risk mitigation strategy organizations can implement.

- Schedule recurrent vulnerability patching at least once a month to ensure consistency and reduce the time required to address security vulnerabilities.
- Dedicated patch management solutions or configuration management tools can help track vulnerabilities, prioritize patches, and automate deployment to keep all operating systems and software up to date.

WatchGuard Technologies, Inc. Page 24 of 33



Report 1 May 2023 – 19 June 2023

DETAILS AND RECOMMENDATIONS

2.8 End-of-Life Software Detected

End-of-Life (EOL) software has reached the end of its support or maintenance period. This means the vendor no longer provides updates, bug fixes, and technical support for a specific version. The EOL stage usually occurs when software is considered outdated, not viable to support, or when vendor resources are focused on newer versions or entirely new products. EOL software is often used as an attack vector by attackers because it no longer receive critical security patches.

Because the presence of EOL software increases the organization's cybersecurity risk, it can also raise insurer concerns and affect cyber insurance terms, either by significantly limiting or excluding coverage altogether.

The assessment has identified that these endpoints have software programs installed that are already or will soon be in the EOL stage.

Most Common End-of-life Software Detected

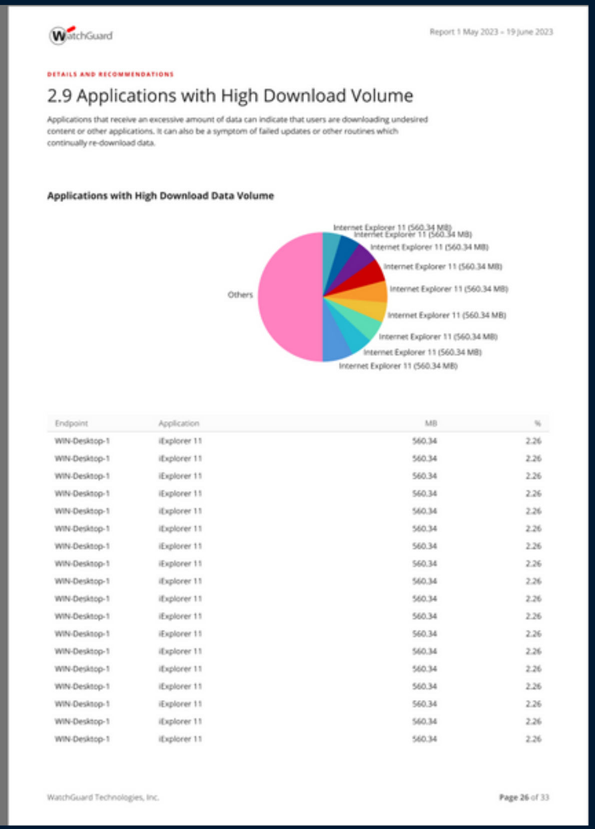
.NET Framework 3.0 (x64)
Microsoft Visual C++ 2008 SP1 Redistributable
Visual C++ 2005 Redistributable (x64)
Microsoft Silverlight 5
Microsoft Silverlight 5 (x64)
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
Endpoints

Recommendations

EOL software could put your data and systems at risk, impacting your cybersecurity posture. It is important to stay up to date with software lifecycles and plan accordingly to ensure continued functionality, support, and security.

- Restrict the corporate software suite as much as possible to programs that are regularly patched.
- Uninstall any EOL software not in use.

WatchGuard Technologies, Inc. Page 25 of 33



Report 1 May 2023 – 19 June 2023

DETAILS AND RECOMMENDATIONS

2.9 Applications with High Download Volume

Applications that receive an excessive amount of data can indicate that users are downloading undesired content or other applications. It can also be a symptom of failed updates or other routines which continually re-download data.

Applications with High Download Data Volume

Internet Explorer 11 (560.34 MB)
Internet Explorer 11 (560.34 MB)
Internet Explorer 11 (560.34 MB)
Internet Explorer 11 (560.34 MB)
Internet Explorer 11 (560.34 MB)
Internet Explorer 11 (560.34 MB)
Internet Explorer 11 (560.34 MB)
Internet Explorer 11 (560.34 MB)
Internet Explorer 11 (560.34 MB)
Others

Endpoint	Application	MB	%
WIN-Desktop-1	iExplorer 11	560.34	2.26
WIN-Desktop-1	iExplorer 11	560.34	2.26
WIN-Desktop-1	iExplorer 11	560.34	2.26
WIN-Desktop-1	iExplorer 11	560.34	2.26
WIN-Desktop-1	iExplorer 11	560.34	2.26
WIN-Desktop-1	iExplorer 11	560.34	2.26
WIN-Desktop-1	iExplorer 11	560.34	2.26
WIN-Desktop-1	iExplorer 11	560.34	2.26
WIN-Desktop-1	iExplorer 11	560.34	2.26
WIN-Desktop-1	iExplorer 11	560.34	2.26
WIN-Desktop-1	iExplorer 11	560.34	2.26
WIN-Desktop-1	iExplorer 11	560.34	2.26
WIN-Desktop-1	iExplorer 11	560.34	2.26
WIN-Desktop-1	iExplorer 11	560.34	2.26
WIN-Desktop-1	iExplorer 11	560.34	2.26
WIN-Desktop-1	iExplorer 11	560.34	2.26
WIN-Desktop-1	iExplorer 11	560.34	2.26
WIN-Desktop-1	iExplorer 11	560.34	2.26

WatchGuard Technologies, Inc. Page 26 of 33

OX IT Solutions Ltd

Remediation

- **If you'd like to remediate the risks found in the Assessment**
  - We can provide an EPDR trial, if required
  - Restore default protection settings

- **Actions**
  - Malware, PUPs and Exploits will be automatically removed with the proper configuration
  - We can activate a Patch Management trial and deploy patches for detected vulnerabilities
  - Leverage product features (Device Isolation, Scan tasks, Program Blocking, etc.) to contain and remediate other Critical or High risks

- **Combine WatchGuard solutions to mitigate risks in the long run**
  - Choose the right Endpoint Security base product for the specific implementation scenario
  - Endpoint Security Modules

How much does it cost?

It is absolutely free and non-intrusive!

Get in touch with us to find out more!

www.oxitsolutions.co.uk
sales@oxitsolutions.co.uk
01865 594930

WatchGuard

OX IT Solutions Ltd