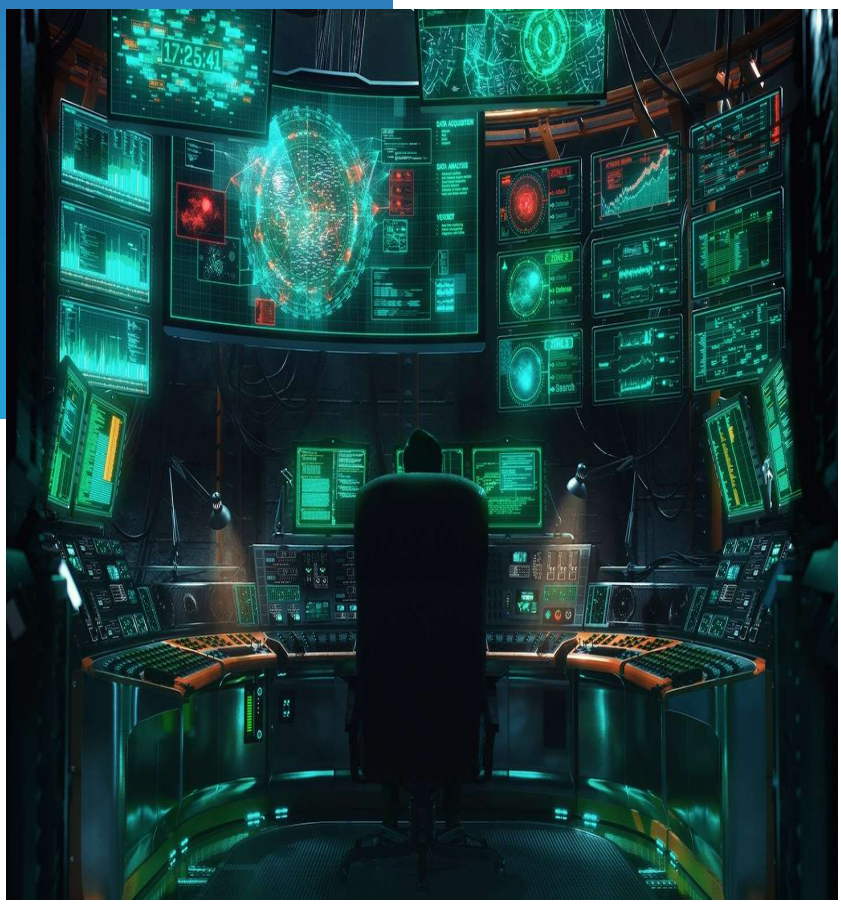


Direct iT EDR
WHY ANTIVIRUS IS NOT ENOUGH

Whitepaper
January 2020
By Patrick Engelman

Greenwood Industries – Worcester, Massachusetts

Greenwood Industries is one of the premiere commercial roofing contractors in New England – their projects have included the Massachusetts State House, Logan Airport, and the TD Bank Garden among many others.

Greenwood's focus is on roofing, not computer infrastructure – while they have one of the best roofing design and engineering teams in New England, they do not have an in-house IT department.

The Petya Threat:

Petya is a dark-web-based ransomware affiliate network and ransomware virus generator.

- Petya uses a **unique virus for every single infection** (they generate thousands per day) to avoid Antivirus
- Petya's criminal **affiliate program** allows independent hackers to help spread the virus for a percentage of the ransom
- Petya specializes in rapidly spreading across networks and disabling backups to make recovery impossible
- Petya **ransom amounts have been steadily rising** and are frequently 5-6 figures

One day, three Greenwood Industries employees received a very convincing email attachment from a trusted customer. It came from the customer's real email address, with authentic signature and tone.

The email was so convincing that all three employees opened the attachment, not realizing that their customer's email had been hacked and that the attachment was in fact the Petya ransomware virus.

If Greenwood had been relying on traditional antivirus, their data could have been lost. Once encrypted the only options for recovery would have been either to pay the ransom or start a lengthy process restoring backups (and hoping the hackers had failed at disabling or deleting those backups).

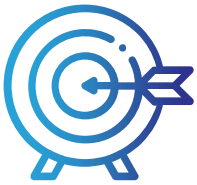
If Greenwood had been relying on traditional antivirus, their data could have been lost.

EDR SAVES THE DAY

Instead of an in-house IT department, Greenwood Industries has been working for the past 14 years with Direct iT out of Waltham, MA, an MSP and outsourced IT provider that has become Greenwood's trusted IT team.

As part of their managed services support program, Direct iT had proactively switched Greenwood from traditional antivirus to EDR (Endpoint Detection and Response). EDR is latest generation of security software that uses artificial intelligence, the cloud, and pro-active remediation/response techniques to detect and stop threats that traditional AV can't.

As soon as the 3 users opened the ransomware e-mail attachment, Direct iT EDR's artificial intelligence detected something unusual happening and notified Direct iT's Security Operations Center (SOC). The EDR software also automatically disconnected the 3 affected machines from the network and Greenwood got a call from Direct iT engineers, who were able to clean the machines and reconnect them without incident.



Artificial Intelligence Malware Detection

AI looks at patterns and behaviors of all software on your system to detect anomalies

Managed Security Team Response

Direct iT's security team trains this AI to customize it for your network and responds quickly to any threats

Pro-Active Remediation

Pro-active EDR tools allow infected systems to be isolated instantly – part of Direct iT's overall pro-active approach to security.