Community Newspaper Group Gives Threats Nowhere to Hide

Check Point SandBlast Agent protects critical CNG assets from advanced malware without impacting employee productivity

Customer Profile

Community Newspaper group provides local news to citizens throughout western Australia.

Challenge

- Gain better visibility and actionable data for fighting advanced threats on laptops and desktops
- Minimize security impact on users
- Simplify and centralize threat monitoring, management, and reporting

Solution

- Check Point SandBlast Agent with Threat Emulation and Forensics

Benefits

- Detected and blocked numerous advanced threats that previous solutions missed
- Forensics capability provided full visibility to identify threats to enhance overall security posture
- Maintained users' productivity while providing increased security at the endpoint

> "SandBlast Agent found multiple threats within the first days we deployed it. Not only was Check Point more effective in identifying sophisticated attacks—it also eliminated them before they could cause damage. It actually does its job better than we expected. It's fantastic."
>
> — Michael Brine,
> Infrastructure Manager, Community Newspaper Group (CNG)

Overview

Community Newspaper Group

The Community Newspaper Group's (CNG's) seventeen regional newspapers and associated websites provide readers in Western Australia with the latest local news, sports, entertainment and more.

Business challenges

No Time for Downtime

More than 700,000 readers rely on their daily Community Newspaper Group content to stay informed about local news and events. In today's fast-moving publishing world, readers expect near real-time information even at the local level, so downtime that affects CNG reporters and employees or the network is not an option. Advertising is still the primary revenue source for CNG, so any interruptions that could prevent timely rollout of physical or online editions translate to lost revenue and potentially dissatisfied clients.

Until recently, Community Newspaper Group protected end-user systems and digital assets with Trend Micro and Microsoft security solutions. However, the software was aging, and IT needed better visibility into threats. The existing solutions required IT to navigate multiple dashboards to gather data from various areas of the network and then piece together a picture of what was happening.

"Visibility is everything,"' said Michael Brine, Infrastructure Manager, Community Newspaper Group. "If you know about a problem, you can do something about it. But we suspected that there were vulnerabilities and events we didn't even know about."

Solution section

Beyond Basic Protection

At the start of his search, Brine evaluated multiple security vendors in search for a new antivirus solution. At this time, he also looked to upgrade his existing Check Point Firewall and chose Check Point's 4600 Appliance with Next Generation Threat Prevention. It was then that Brine learned about SandBlast Agent for endpoint security. His task of selecting the right advanced endpoint security solution became much simpler.

Having had great experience with Check Point Threat Prevention solutions on the network side, Brine felt confident that SandBlast Agent was the right choice to provide him with a deeper level of protection and visibility into threats on his endpoints that he needed.

> "Check Point delivers visibility," said Brine. "Without Check Point, it would have taken us hours to do the work for every incident to determine exactly what happened and what we need to do to resolve it. That is now almost entirely automated, saving us significant time every day."
>
> — Michael Brine

Advanced Endpoint Protection

CNG chose Check Point SandBlast Agent to protect the company's desktop and laptop systems. SandBlast Agent uses a complete set of advanced endpoint protection technologies to secure CNG's users from threats, regardless of whether they are connected within their corporate network or working remotely.

Community Newspaper Group has seen an increase in attacks that use social engineering techniques such as phishing to deliver malware, including recent ransomware. SandBlast Agent helps CNG detect and block these attacks, whether originating from email, removable media, or web-based threats. By blocking any command and control communications, it also limits damage in case of infection, by preventing movement of sensitive information externally and restricting spread of the attack to other systems.

Community Newspaper Group relies on the Threat Emulation capability within SandBlast Agent to discover malicious behavior—even new, unknown malware and targeted attacks—preventing infection by quickly inspecting files in a virtual sandbox. It even uncovers threats hidden in SSL and TLS encrypted communications, while providing protection for the various files types used to share information at CNG, including Microsoft Word and Excel and Adobe PDF.

Files that look suspicious are flagged for deeper analysis. Threat Emulation sandboxing detects and stops attacks before they have a chance to evade detection, preventing systems from becoming infected. In cases where new malware is discovered, Threat Emulation sends a signature to the Check Point ThreatCloud database, which documents and shares information on the newly identified threat.

Improved Threat Visibility

SandBlast Agent's forensics capability gives Brine and his team a deeper understanding of security events by automatically generating an incident report when any abnormal activity is tracked on any of their systems. The report summary provides actionable attack information, including evidence of malicious events, attack entry point, elements used in the attack, scope of damage, and data about devices that are infected. The combination of having the relevant attack diagnostics and visibility enables Brine and his team to respond quickly and remediate their systems in the case of a security event.

> “SandBlast Agent is able to analyze all content in the cloud, without interfering with the user's experience. Now, we have both better protection and less impact on users.”
>
> — Michael Brine

Benefits section

Prevents Advanced Threats and Attacks

Check Point SandBlast Agent replaced CNG's Trend Micro solution. Testing and rollout to all endpoints took only two weeks, and during the rollout of SandBlast Agent, Brine and his team found many more infections than the prior solution had recognized.

“SandBlast Agent found multiple threats within the first days we deployed it,” said Brine. “Not only was Check Point more effective in identifying sophisticated attacks—it also eliminated them before they could cause damage. It actually does its job better than we expected. It's fantastic.”

Full Visibility into Security Events on Endpoints

SandBlast Agent forensic capabilities gave Community Newspaper Group the clear visibility they wanted. The software monitors and records all endpoint events, including files affected, processes launched, system registry changes, and network activity. It also makes sure that data is available after completed attacks—even those that remove files and other evidence left on the system.

The comprehensive incident summary provides actionable attack information for Brine. For example, he now can document evidence of suspicious behavior detected throughout the attack lifecycle. He can see how the attack entered the network, how it was launched, and the methods used. He knows the type of damage that occurred, if data was stolen, which systems were affected, and how they were affected.

“Check Point delivers visibility,” said Brine. “Without Check Point, it would have taken us hours to do the work for every incident to determine exactly what happened and what we need to do to resolve it. That is now almost entirely automated, saving us significant time every day. With SandBlast Agent and the Check Point 4600 Appliance, I have phenomenal visibility.”

Easy to Use

Because the solution is completely integrated, everything can be viewed from the same console. CNG can deploy SandBlast Agent to new endpoints, manage policies, access event logs and incident reports, and troubleshoot all through the Smart-Center dashboard.

Minimal Impact on Performance

“With our previous solution, users frequently complained that performance suffered from the overhead of local processing to analyze threats,” said Brine. “SandBlast Agent is able to analyze all content in the cloud, without interfering with the user’s experience. Now, we have both better protection and less impact on users.” He also reports that the SandBlast Agent has dramatically reduced the number of infections on their endpoints.

“This is especially helpful for our reporters,” said Brine. “They often have to gather information from dodgy sites that they never would otherwise visit, but they know that specific files that could contain malware will be evaluated first. This allows our highly mobile workforce to manage their business with complete confidence.”

Next Steps

Brine is a big fan of Check Point solutions for Community Newspaper Group, and he plans to activate more capabilities as time goes on.

“We’d like to implement encryption on our endpoints and perhaps add network-level threat emulation and extraction capabilities,” he said. “Meanwhile, Check Point just quietly does its job, and I have deep visibility into everything. Visibility is the most critical thing for helping me keep our users and data safe.”

For more information, visit
www.checkpoint.com/sandblastagent

Check Point
SOFTWARE TECHNOLOGIES LTD