

# Koch Media Levels Up Security to Protect Intellectual Property Against Attackers

Check Point SandBlast Secures Game Code and Centralizes Security Management

## KOCH MEDIA

### Customer Profile

Koch Media is a German producer and marketer of digital entertainment products.

### Challenge

- Secure applications and intellectual property, such as game code
- Stop malware and a range of zero-day threats
- Centralize and simplify management across 25 locations

### Solution

- Check Point SandBlast Zero-Day Protection

### Benefits

- Stopped threats that otherwise would have not been discovered
- Gained consistent end-to-end protection across all company locations
- Secured applications with fine-grained policies to protect code from unauthorized users
- Saved hours of time through automation and centralized visibility

“Check Point secures our ‘last mile’ of file delivery. We gained end-to-end infrastructure protection with the ability to see what SandBlast blocks. It’s highly effective.”

— Liang Zhang, Director of Networking and Security, Koch Media GmbH/Deep Silver

## Overview

### Koch Media GmbH

Koch Media is a leading independent producer and marketer of digital entertainment products in Europe and North America. It distributes movies, video games, and software products, and publishes games under the Deep Silver label.

## Business Challenges

### Protecting Intellectual Property—and Revenue

Koch Media is a trusted publisher and marketer for a wide range of media products, including games. Moving products through development with multiple partners can potentially expose them to risk. For example, games are unprotected code while they are being developed. If a developer is attacked, code could be lost or exposed to the world, which would mean loss of revenue and trust. Securing game code, sensitive business data, and other assets is challenging across more than 25 locations—each of which has its own security rules and policies.




---

“Check Point SandBlast was easy to deploy. It automatically joined our secure VPNs that connect each location and gives us end-to-end protection against attackers.”

— Liang Zhang, Director of Networking and Security, Koch Media GmbH/Deep Silver

---

In the past, Koch Media used Cisco Adaptive Security Appliances (ASA) in each location. Company locations often need to change a firewall rule to accommodate a business process. For example, when the Koch Media office in Milan needed to use a specific web conferencing solution to collaborate with a partner, the IT team had to physically go to the firewall, change the rule, and manually reconfigure the firewall. With only a Command Line Interface (CLI), the team had to work through 100 lines of code just to change one line. Because this was a manual process, it was open to human error, and requests for changes arrived daily.

Sharing large files safely also became a concern. As applications are now critical, securing ports or IP addresses is no longer enough. Koch Media needed the ability to secure the application layer, especially with assets such as game code. In addition, the IT team was seeing a growing amount of malware that its antivirus missed.

“We needed protection against zero-day threats,” said Juri Vaisman, Director of IT International at Koch Media GmbH/Deep Silver. “We also needed to centrally manage all locations and the flexibility to change rules without disrupting the network by having to reconfigure firewalls.”

## Solution

### Simple, Effective, and Pervasive

Koch Media already had deployed Check Point Next Generation Threat Prevention (NGTP) with multi-layered protection from known, signature-based threats. With Check Point SandBlast Zero-Day Protection, it gained real-time protection against zero-day attacks using sandboxing and Threat Extraction.

“Check Point SandBlast was easy to deploy,” said Liang Zhang, Director of Networking and Security at Koch Media GmbH/Deep Silver. “It automatically joined our secure VPNs that connect each location and gives us end-to-end protection against attackers. It also gives us a number of other controls that we needed to better secure our stock in trade—applications.”

## Benefits

### Powerful Protection from Otherwise Unseen Threats

SandBlast Threat Emulation performs real-time sandboxing capabilities, quickly inspecting files and running them in a virtual environment to discover and block malware. SandBlast Threat Extraction removes exploitable content—such as active content and embedded objects—from documents and delivers a safe copy of the file to users. Check Point enables the IT team to control the level of security they need for different file sizes, which is critical for gigabyte-size media files.

“Check Point secures our ‘last mile’ of file delivery,” said Zhang. “We gained end-to-end infrastructure protection and the ability to see what SandBlast blocks. It’s highly effective.”



“Central management is a huge time-saver to reimage machines, and we have more time to focus strategically on threats instead of having to constantly react.”

— Liang Zhang, Director of Networking and Security, Koch Media GmbH/Deep Silver

## Securing Applications for Greater Peace of Mind

SandBlast Application Control capabilities give the team granular control over applications, such as games. They can create specific policies based on many different attributes to make sure that only authorized users can see code. SandBlast URL Filtering also controls access to millions of websites, preventing users from going to malicious sites to support productivity and security policies.

## Higher Management Efficiency

The IT team gained its wish with centralized management. Check Point SmartEvent consolidates monitoring, logging, reporting, and event analysis into a single console so that they can see attack data from all of their locations. The team quickly and easily handles requests from all of the company’s locations, and changes are as simple as drag and drop.

“Central management is a huge time-saver,” said Zhang. “We rarely have to reimage machines, and we have more time to focus strategically on threats instead of having to constantly react.”

## Next: Growth and Expansion

The company is growing rapidly, adding locations and staff. With growth comes a larger attack surface. Vaisman is considering adding Check Point SandBlast Agent with Threat Emulation and Forensics to provide another layer of protection on company endpoints. SandBlast Agent will give the team even greater visibility into incidents, along with attack diagnostics and actionable attack information.

“We need to support growth without compromising protection,” said Vaisman. “It’s simpler to achieve that goal and protect intellectual property using Check Point.”



For more information, visit [www.checkpoint.com/sandblast](http://www.checkpoint.com/sandblast)