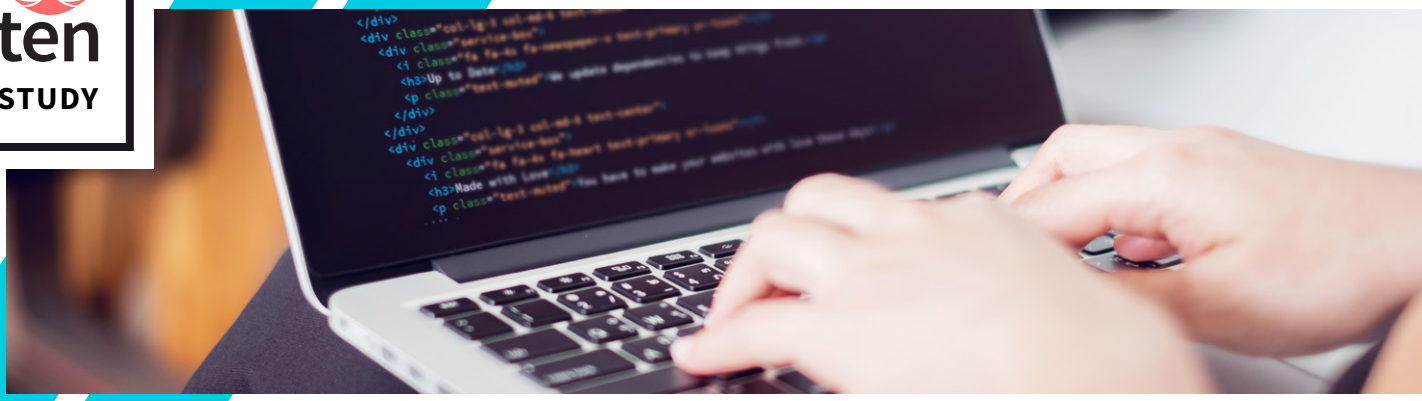
ziften
CASESTUDY



VISUAL SOFTWARE COMPANY

Software Company Improves Endpoint Protection and Real-Time Visibility

Challenges:

- Need to improve threat detection and sophistication of overall security program.
- Lack of in-depth endpoint visibility, both endpoint activities and threats.
- Lack of threat contexts – alerts without meaning, insight, or resolution guidance.
- Inability to prioritize actions by threat level.

Benefits:

- Implemented continuous threat detection, hunting and response for first time.
- Now detecting suspect and malicious user and file behaviors with machine learning that was previously undetected.
- Security analysts now get immediate access to incident response data.

Seeking Superior Endpoint Protection

When companies want to develop impactful videos or images to share their knowledge with others, they look this visual communications software company. The customer develops screen-shooting, screen-casting, and video editing software for Windows and Mac systems. Founded in the 1980s, they pioneered the revolutionary idea of capturing screen content for better communication. Educational institutions, government agencies, and businesses around the world choose them as their go-to company for visual communication. Today, the customer is the world's #1 source for visual communication software.

The customer's IT and security teams understand the complexity of the threat landscape and the daily challenge of balancing users' needs and security concerns. They wanted to increase the sophistication of their security program to better protect the company's assets. Realizing visibility is the key to staying ahead of the bad guys, the team conducted an extensive review of leading endpoint protection products, specifically focusing on those with endpoint detection and response (EDR) capabilities. "We wanted a solution that would allow us to detect, view, investigate, and respond to advanced cyber-attacks," said the IT Security Manager. "We needed better insight into endpoint activities on our Windows and Mac environments and wanted to be able to continuously monitor and capture data on all endpoint activities."

Visibility, Context and Control

After in-depth evaluations of multiple solutions, the security team chose Microsoft Windows Defender ATP combined with Ziften Zenith because of the products' advanced endpoint detection and response capabilities and platform support. Windows Defender ATP is Microsoft's post-breach analysis service that uses machine learning and expert analysis for detection, investigation, response, and forensics for Windows environments, while Ziften Zenith integrates with Windows Defender ATP to provide protection for macOS and Linux systems. "Tight integration of the products provides us a 'single pane of glass' to manage security across our Windows and Mac endpoints," said the IT Security Manager. Integration for visibility and incident response purposes was important. "When you have a security problem to deal with, you don't want to waste time jumping between multiple consoles. Now we are able to proactively deal with problems much faster."

"Ziften's Zenith seamless integration with Windows Defender ATP allows us to monitor and visualize threats across all platforms in real-time through a single pane of glass."

Customer's Security Analyst

Detecting Malicious Software and Behaviors

In addition to providing information about endpoint activity, Windows Defender ATP and Ziften Zenith deliver insights into what devices are connected to the network and what they are doing, as well as how many users are running or consuming each specific application. Aside from being able to detect malicious software, the joint security solution also alerts on malicious behaviors – helping to discover hidden threats that, until now, went undetected by their traditional endpoint security measures.

The products' user and entity behavior analytics make it possible to detect malicious actors that have illicitly gained access to a system, application, or data with the intent of writing and executing harmful scripts. Unlike downloaded malware, which is easily detected, hackers can infiltrate internal systems without being detected. With the right credentials, users and hackers can write scripts that can download and install software, create user accounts, log key strokes, and perform all sorts of acts –including malicious. Only with the use of behavior analytics and machine learning technology can abnormal – potentially malicious – behaviors be detected. "Ziften's ability to detect and alert based upon unusual behavior is a big benefit," said a customer's security analyst.

Optimal Protection, Exceptional Support

The customer's IT and security operations teams were surprised by the increased level of visibility gained with Microsoft and Ziften. "Ziften's Zenith seamless integration with Windows Defender ATP allows us to monitor and visualize threats across all platforms in real-time through a single pane of glass," said the customer's security analyst. According to the customer, a superior product is not the only benefit Ziften provides. "Ziften knows how to deliver on product, promises, and people. We really appreciate the Ziften's straightforward approach to doing business and ongoing commitment to deliver upon their product enhancements." said the IT Security Manager.

ziften