Seattle Theatre Group gets first-rate reviews for network security

Performing arts group mitigates malware-driven network exposures to sites in Russia, eliminates network outages and malware-related endpoint issues

THE CHALLENGE

In theater, the show must go on. If problems arise, the theater's actors, crew, and the business offices do what they can to keep performances running smoothly. When network outages and slowdowns were affecting business operations at Seattle Theatre Group, the Internet service provider and internal SonicWall firewall reported there were no issues. Also concerning was that Symantec Endpoint Protection and Microsoft Windows Defender were not blocking malware from hacking users' workstations and office servers.

Seattle Theatre Group's IT team evaluated alternative network solutions, including ExtraHop Reveal(x), Microsoft Advanced Threat Analytics and Bitdefender Network Traffic Analytics (NTA). For endpoint security, IT considered Malwarebytes, Avast and Bitdefender. Bitdefender rose to the top of the pack with Seattle Theatre Group choosing NTA and GravityZone Business Security Premium..

Michael E. von Kempf, Computer and Information Systems Manager, Seattle Theatre Group, recalls, "Bitdefender's consistent top rankings by security analyst and testing firms such as AV-TEST combined with the user-friendly, Web-centric interface were big factors in our decision. As a small organization with limited funding, we also appreciated that Bitdefender's advanced security was affordable."

THE SOLUTION

Seattle Theatre Group chose Bitdefender Network Traffic Analytics to detect advanced attacks in real time and automate alert triage for incident response across its network of Cisco Meraki access points, switches and firewalls. NTA uses machine learning and behavior analytics with insights from Bitdefender cloud threat intelligence generated by 500 million sensors globally to detect threats.

Bitdefender GravityZone Business Security Premium was selected to protect Seattle Theatre Group's 200 endpoints, including Microsoft Windows and Apple workstations, Windows and Linux servers, as well as virtualized Microsoft Hyper-V servers. Bitdefender also protects

SEATTLE THEATRE GROUP

Seattle Theatre Group presents Broadway theater, concerts, dance, comedy, family engagements, silent film and jazz performances at three Seattle theaters, and delivers performing arts programs to local schools. The non-profit organization also is committed to preserving historic arts buildings, such as the Paramount Theatre in Seattle.

Industry
Entertainment

Headquarters
Seattle, Washington, USA

Employees
200 (IT staff, 1)

Results

- Network outages and slowdowns decreased from once a week to zero
- Isolated and mitigated malware on machines exposing network to sites in Russia
- Malware-related trouble calls occurring three times per week previously, disappeared
- Weekly endpoint security administration reduced from 24 hours to one hour

Seattle Theatre Group's Microsoft Azure cloud endpoints. Applications running on endpoints protected by GravityZone include Microsoft Dynamics NAV ERP, Microsoft Office, Microsoft Active Directory, Adobe Creative Suite, Salesforce and Ticketmaster remote desktop.

In addition, Seattle Theatre Group plans to use GravityZone Patch Management to automate patching of operating systems and applications for improved compliance and efficiency.

THE RESULTS

NTA revealed that users were inadvertently activating malware extensions in Google Chrome and exposing Seattle Theatre Group's network.

"Immediately, NTA showed there was malware embedded in our network that was pinging multiple locations in Russia," says von Kempf. "I mitigated that completely with NTA by isolating machines that were communicating with Russian IP addresses."

For comprehensive analytics, NTA provides the Seattle Theatre Group with access to Bitdefender's massive threat intelligence database to highlight malicious traffic patterns in real time. NTA oversees Seattle Theatre Group traffic involving local machines and machines used by people on tour at local theaters who access the network temporarily. von Kempf values NTA's rich intelligence and ability to sort devices by IP addresses and Windows names for investigations.

von Kempf explains, "NTA's IntelliTriage function prioritizes alerts by four levels so I can identify the ones to analyze first. It also provides an array of investigative tools to track and isolate issues by machine. NTA is a powerful, slick and user-friendly tool that paints an accurate picture of any trouble spots. Already, network outages and slowdowns that were happening once a week on average have dropped to zero."

GravityZone provides Seattle Theatre Group with another layer of security by enabling endpoint protection.

"Before, we were getting three trouble calls a week from users about malware-related issues," notes von Kempf. "With GravityZone, those calls have gone away since GravityZone blocks any malware before it starts affecting user machines."

von Kempf also reports that GravityZone's success in protecting endpoints and easy-to-use interface have reduced the time he spends managing endpoint security from 24 hours to one hour a week.

"Together, NTA and GravityZone improved user experience immensely by increasing trust and comfort in our infrastructure and network," reflects von Kempf. "I'm looking forward to Bitdefender's plans to integrate the GravityZone cloud console with NTA. This will automatically trigger containment actions on endpoints when advanced threats are detected by NTA."

"Immediately, NTA showed there was malware embedded in our network that was pinging multiple locations in Russia. I mitigated that completely with NTA by isolating machines that were communicating with Russian IP addresses."

Michael E. von Kempf, Computer and Information Systems Manager, Seattle Theatre Group

Bitdefender Footprint

- Network Traffic Analytics
- GravityZone Business Security Premium
- GravityZone Patch Management

IT Environment

- Apple Server
- Microsoft Active Directory
- Microsoft Azure
- Microsoft Azure Directory
- Microsoft Hyper-V

Operating Systems

- Apple (Mac)
- Linux
- Microsoft Windows

13042022-Bitdefender-CaseStudy-STG-crea6103-a4-en_EN