CYLANCE

CASE STUDY HEALTH INSURANCE

Health Insurance Company Takes on Cybersecurity

INDUSTRY
Health
Insurance

ENVIRONMENT
- Over 7,000 endpoints

CHALLENGES
- Replace the incumbent signature-based antivirus solution, EDR, and host IDS/IPS products with endpoint defenses based on AI/ML predictive technologies
- Prevent the execution of advanced malware, and script-based and fileless attacks
- Comply with legal and regulatory requirements to secure subscribers' personal health information and personally identifiable information

SOLUTION
- Decommission existing endpoint security solutions and operationalize CylancePROTECT® on all endpoint systems

The Company

A privately-held health insurance company serving more than 30 million members at locations throughout the United States.

The Situation

The healthcare industry has become a rich target of opportunity for attackers and identity thieves seeking unauthorized access to patients' highly-sensitive personal health information and personally identifiable information.

The CISO of this health insurance company was acutely aware of the firm's susceptibility to a data breach or ransomware attack and the damage this would inflict on the company's business operations and brand reputation. Consequently, he felt a sharp sense of urgency to replace the aging signature-based endpoint defenses with a solution capable of proactively preventing advanced persistent threats and zero-day exploits. According to the CISO, "We decided to pursue a bifurcated threat management strategy, with an endpoint detection and response component for retrospective analysis and remediation, and an endpoint protection platform for proactive prevention. Given the vulnerability of our current defense posture, we decided to focus first on prevention."

The CISO and his team identified three key requirements for their new endpoint protection platform:

- Malware Execution Control: The solution must prevent both file-based and fileless malware from executing on the company's Windows and Linux-based systems
- Script Control: The solution must block the execution of malicious Active Scripts concealed in weaponized attachments and scripts that exploit common system services such as PowerShell
- High Performance and Administrative Efficiency: The solution must not degrade system performance or require frequent updates to remain effective

The Process

With requirements in hand, the CISO and his team were ready to assess candidate solutions. They began by limiting the field to products with proven capabilities for pre-execution prevention across a wide variety of threats. The selected provider would also have to demonstrate a solid reputation for post-sales service and support. "We quickly winnowed the list down to Cylance and another next-gen AV solution, and invited both companies to compete in a two-phase proof of concept evaluation," said the CISO.

In Phase 1, the Proof of Concept (POC) team installed the agent software for CylancePROTECT and the competitor's software on a representative sample of Windows and Linux machines. Next, they executed a variety of test cases to assess each product's compatibility and performance. "Both products passed those tests with flying colors," said the CISO. In Phase 2, the company, in partnership with one of its service providers, assessed efficacy by exposing CylancePROTECT and the competitor's software to a series of real-world attack scenarios. According to the CISO, "CylancePROTECT was clearly superior in both the robustness of its artificial intelligence technology and its capabilities for pre-execution prevention. In our tests, CylancePROTECT instantly detected and blocked every malicious script and executable we threw at it. It was an impressive performance."

The POC team also appreciated the efficient design and workflow of CylancePROTECT's configuration and management features. "We found the process of defining policies and applying script and executable blocking controls to be both logical and straightforward. This gave us confidence we'd be able to efficiently deploy and manage CylancePROTECT on our own," said the CISO. After completing the POC, the CISO and his team selected CylancePROTECT as the company's new endpoint protection platform.

The Results

The CISO and his SOC team mapped out an orderly transition plan that began with decommissioning the company's existing antivurus solutions and rolling out CylancePROTECT on all 7,000 endpoints, with malware prevention fully enabled, but script and memory protection configured in Alert Mode only. Once that deployment completed successfully, the team enabled CylancePROTECT's advanced script blocking and memory protection features on all end-user machines.

According to the CISO, "Our business users appreciate how CylancePROTECT works quietly in the background without slowing down their systems or requiring frequent disc scans. Our SOC team is pleased that we no longer have to devote time and effort to manage signature updates. But the real win is the dramatic risk reduction we've achieved by adopting a prevention-first security posture. Thanks to CylancePROTECT, we're confident that our data and systems are truly secure."

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
400 Spectrum Center Drive, Irvine, CA 92618

20180822-1011