Organization
Customer: ECI
Site: http://ecitele.com
Industry: Telecommunications
Headquarters: Tel Aviv, Israel
Employees: 1,800

Challenges
ECI needed a technology to accurately detect endpoint-targeted attacks, which could be implemented and utilised without the need for additional resources (to recruit more staff or obtain additional endpoint agents).

Solutions

- Symantec Endpoint Protection
- Symantec Advanced Threat Protection

Benefits

- Increased incident response capabilities without deploying a new agent
- Easy prioritisation of incidents through integration with Symantec Endpoint Protection
- Investigation of advanced attack incidents using the existing team
- Single product that enables detection, investigation, and remediation across control points
- Single console to manage global sites
- Integration with existing SIEM and IT Ticket systems

ECI
THE ELASTIC NETWORK

ECI

ECI takes security to the next level with Symantec Advanced Threat Protection.

ECI offices are located all over the world. The IT security team recognised that they needed a new generation of technology to detect the latest advanced threats. They decided to trial Symantec Advanced Threat Protection: “to see if it lived up to the promise of a solution that could address their concern of advanced threats.”

The trial showed value very quickly, by detecting new vulnerabilities that other systems did not. The built-in integration with Symantec Endpoint Protection made ongoing use very easy. This led ECI to a decision to proceed and implement Symantec ATP for Endpoint and Network.

ECI is a global provider of ELASTIC network solutions to CSPs, utilities as well as data center operators. Along with its long-standing, industry-proven packet-optical transport, ECI offers a variety of SDN/NFV applications, end-to-end network management, a comprehensive cyber security solution, and a range of professional services. ECI’s ELASTIC network solutions ensure open, future-proof, and secure communications. With ECI, customers have the luxury of choosing a network that can be tailor-made to their needs today as well as be seamlessly and cost effectively upgraded to future requirements.

As ECI Telecom’s Global Chief Information Security Officer, Dor Liniado manages information security for its global network including data centres, international branches and R&D centres. This means Liniado’s role is far reaching. He and his team are responsible for securing file transfers, preventing data breaches, reviewing contracts and their requirements, complying with supplier and customer information and security specifications.

Tactical and strategic challenges

Such a remit brings many tactical and strategic challenges. For example, finding ways to increase end-user awareness about information security: “Previously you could surround yourself with infinite layers of systems and solutions. However, without end-user awareness and education, you’ve got a problem,” explains Liniado. Today, Symantec Advanced Threat Protection (ATP), is installed in 99.5% of ECI’s endpoint terminals providing additional security layers even in situations where the lack of employee awareness has an impact.

> Within a week of the initial deployment, Symantec ATP Network provided additional threat recognition capabilities. We were able to increase visibility and capabilities of Symantec ATP by simply integrating the tool into Symantec Endpoint Protection and without the need for additional agents.
>
> —Dor Liniado
> Global CISO
> ECI

Another challenge is overcoming the lack of resources committed to information security. There is always a balance between solutions and resources.

Even when suitable security systems are in place, there is always a question of prioritisation, helping existing teams be more effective in prioritising, investigating and remediating advanced threats in a simple vital way.

The value of Symantec ATP

Due to the trial's success ECI's account team then sought out customers that could join the controlled release and provide feedback about ATP working with their particular systems.

As an early adopter with a unique aptitude and track record for incorporating and evaluating new technologies, ECI was able to provide valuable assessments and constructive observations to the Symantec ATP product management team.

The ECI team installed Symantec ATP in August 2015 and it was soon operating effectively. "Full deployment of ATP capabilities was possible within an hour and we were able to install it ourselves. The simplicity to install and ease of use and speed of integration with our existing environment is one of the product's strengths," Liniado enthuses.

"ATP goes beyond Symantec's endpoint protection. We enjoyed the solution's capabilities. Now we have more visibility into which files might be infected or how many stations have been in contact with a particular source. ATP does this quickly and also allows you to quarantine these stations while performing remediation from the same management console."

"ATP also goes from identifying multiple incidents, to better understanding their implications. In addition, based on machine learning technology, ATP prioritises alerts, enabling us to focus our efforts more efficiently," he continues.

Now, when Liniado's team members want to know if they are affected by a threat, they can query ATP for Indicators of Compromise (IOC) and get results within a few seconds. "These capabilities are very impressive," says Liniado.

Two innovative technologies at the core of ATP

Two innovative technologies are at the core of ATP: Symantec Cynic™ and Symantec Synapse™. Cynic is a cloud-based dynamic malware analysis service that provides the ability to detect advanced threats.

'Sandbox' analysis products were developed to focus on offering a variety of virtual machines or customer-specific images to detonate and detect malware. Over the years online threats have become increasingly sophisticated, and the products and tools that were once used and trusted may no longer be the right solution. Today, Cynic uses a suite of analysis technologies, coupled with Symantec's global intelligence and analytics data to accurately detect malicious code, and is designed to avoid detection in virtual machine environments.

> “Full deployment of ATP capabilities was possible within an hour and we were able to install it ourselves. The simplicity to install and ease of use and speed of integration with our existing environment is one of the product’s strengths.
>
> —Dor Liniado
> Global CISO
> ECI

Synapse technology prioritises what matters most. This allows security analysts to zero in on just those specific security events of importance instead of manually correlating alerts duplicated across various systems. Synapse will also aggregate and correlate all suspicious activity across endpoints, networks, and email. Fusing this with data from Symantec’s Global Intelligence Network—the world’s largest civilian intelligence network—to identify and prioritise those events that are of greatest risk. This provides a single comprehensive view of all attack activity across control points enabling users to visualise and remediate all related attack artefacts such as files, email or IP addresses.

Identification and remediation capabilities improved

Symantec ATP added to ECI’s already strong identification and remediation capabilities. We are consistently improving our threat detection abilities,” Liniado concludes.

For more Information:

Contact your local Symantec Sales Representative or Business Partner, or please visit: www.symantec.com/products/advanced-threat-protection.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world’s leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec’s Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world’s largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit **www.symantec.com** or connect with us on **Facebook**, **Twitter**, and **LinkedIn**.

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com