# Play Offense
# Symantec Advanced Threat Hunting

A cyberattack can have far-reaching effects across an organization, and attacks are often not detected for weeks or months. Despite the growth in new technologies to speed identification of threats, more than 60 percent of companies rate themselves as less than highly effective in detecting malicious activity within their organizations, and most state that on average, it takes in excess of 100 days to find out that their organization is under attack.[1]

Simultaneously, the stakes are moving higher for companies in terms of loss of revenue, reputation, and intellectual property. When attackers remain on the network, they are able to surveil the environment, determine the nature and location of important assets and build a strategy for a bigger and even more meaningful attacks.

That is why combatting threats has become more critical than ever. Symantec's new Advanced Threat Hunting (ATH) offering combines Symantec Security Analytics (formerly Blue Coat), SSL Visibility, and Malware Analysis along with Symantec Incident Response to perform an Advanced Threat Hunt. Symantec's Advanced Threat Hunting service provides companies confidence that they can detect and eliminate hidden attacks before they escalate.

## Play Offense

Advanced Threat Hunting

- Symantec Security Analytics
- World's Largest Intelligence Network
- Experienced Incident Responders
- Existing Threats Identified & Eradicated

### Preventive Incident Response

Regularly hunting for threats helps to establish a consistent, known secure state for your network.

### Don't Wait For an Incident

Identify and eradicate existing compromises before they become a major data breach.

### Reduce Breach Response Costs

Compromises are common and inexpensive to remediate. The average cost of a breach is $4 million.

Identify threats early to avoid high incident response costs.

[1] The State of Malware Detection and Prevention, Ponemon Institute, 2016.

## What is Advanced Threat Hunting?

Threat hunting is a proactive approach to threat detection. It focuses on actively scouting for bad actors and malicious activity on a network – rather than waiting for an incident to happen. Symantec Incident Response uses tools similar to those used in an incident investigation, including its technology, intelligence, and professional expertise to hunt for threats on your network. Symantec's Advanced Threat Hunt service is an Incident Investigation without a known incident.

It leverages:

- The Symantec Security Analytics and Malware Analysis solutions to analyze network traffic for Indicators of Compromise (IOCs) and anomalies.
- Threat intelligence feeds built into the Symantec platform and the Symantec Global Intelligence Network, including DeepSight Intelligence and DeepSight Managed Adversary Threat Intelligence (MATI).
- The anomaly detection feature of Symantec Security Analytics to scan for statistical anomalies, which are analyzed in depth.
- Symantec's Self-Service Evidence Collection Tool and analysis toolset to analyze suspected compromised hosts, when necessary.

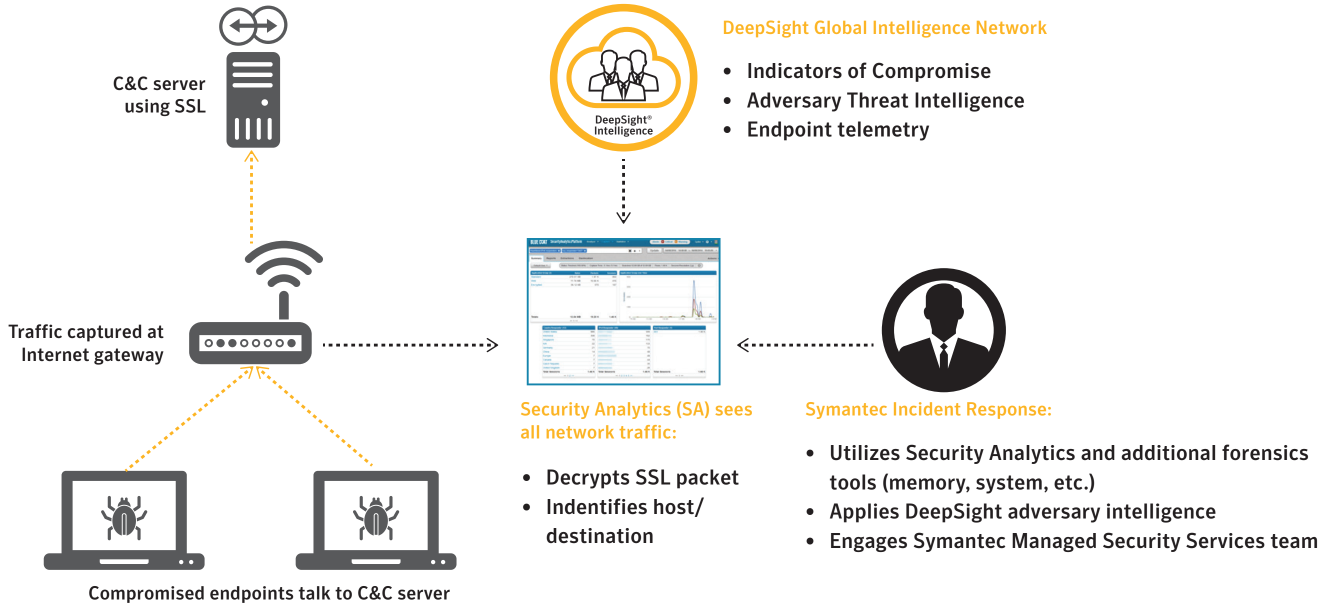
## What Advanced Threat Hunting Does for Organizations

By finding and eradicating existing threats on the network and making security policy and control recommendations based on found threats, threat hunting improves network security posture, reducing overall security risk. Advanced Threat Hunting provides:

- **Preventive incident response** – Regularly hunting for threats helps to establish a consistent, secure state for your network.
- **Insight into threats that pose a risk** – Instead of waiting for an incident, companies can identify and eradicate existing compromises before they become a major breach.
- **Reduced breach response costs** – The average cost of a breach is $4 million. By addressing compromises before they become full-blown, remediation costs are reduced or eliminated altogether.

## Finding Hidden Threats

### Symantec Can Pinpoint Threats Missed by Other Technologies



C&C server using SSL

DeepSight Global Intelligence Network

- Indicators of Compromise
- Adversary Threat Intelligence
- Endpoint telemetry

Traffic captured at Internet gateway

Security Analytics (SA) sees all network traffic:

- Decrypts SSL packet
- Indentifies host/ destination

Symantec Incident Response:

- Utilizes Security Analytics and additional forensics tools (memory, system, etc.)
- Applies DeepSight adversary intelligence
- Engages Symantec Managed Security Services team

Compromised endpoints talk to C&C server

## How Advanced Threat Hunting Works

Modern cyber threats have evolved to leverage high-speed connections and secure encryption to infiltrate networks and exfiltrate data. When users click on a malicious link in a phishing email or fall victim to a watering hole attack, the malware infecting their workstations often use SSL/TLS to communicate with the attacker's command and control (C&C) server, allowing covert and remote access to the victim's network to find, collect, and steal data.

Symantec Incident Response deploys Symantec Security Analytics, Symantec SSL Visibility, and Symantec Malware Analysis at the Internet gateway to gain unprecedented visibility into a company's network traffic, allowing Symantec's highly experienced Incident Response investigators to quickly find and eradicate existing network threats. Traffic is decrypted and then scanned using the world's largest collection of attacker IOCs. To further detect the attacker's network activity, data is subjected to heuristic detection rules, automated malware analytics, and an anomaly detection engine with state-of-the-art machine learning capability. When compromised hosts are identified, Symantec Incident Response immediately notifies the customer's IT security staff to implement a containment and eradication plan. Meanwhile, Symantec conducts host-based forensics using its Self-Service Evidence Collection toolkit to perform root cause analysis, identify the scope and severity of the threat, and to recommend improvements to the customer's security posture.

## How to Deploy Advanced Threat Hunting in Your Organization

Symantec's Advanced Threat Hunting is simple to deploy and economical. Leveraging Symantec Security Analytics, SSL Visibility and Malware Analysis, Symantec is able to quickly scope and execute an Advanced Threat Hunt in your organization. Specifics:

- Engagements are scoped on a custom basis to accommodate each company's budget.
- The cost is based on the number of network segments monitored.
- The final report accompanies the assessment and requires an additional 2-5 service days to create, based on complexity.

## About Symantec Cyber Security Services

Symantec Cyber Security Services offers what no other organization can provide – an integrated and purpose-built portfolio of human expertise, advanced machine learning capabilities and technologies and actionable threat intelligence. Each offering in the Cyber Security Services portfolio is designed to integrate with one another and fuel an organization's cybersecurity program with better insight and faster detection and response capabilities across the entire attack lifecycle.

- **Before an attack:** Track and analyze adversary groups and key trends and events around the globe through Symantec's DeepSight Intelligence.
- **During an attack:** Detect targeted and advanced persistent threats and campaigns through Symantec's Managed Security Services.
- **After an attack:** Respond quickly and effectively to credible security threats and incidents through Symantec's Incident Response.
- **Preparation for an attack:** Strengthen cyber readiness across the organization to recognize and prevent advanced attacks through Symantec Cyber Skills Development.

## About Symantec

Symantec Corporation World Headquarters
350 Ellis Street Mountain View, CA 94043 USA
+1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

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.