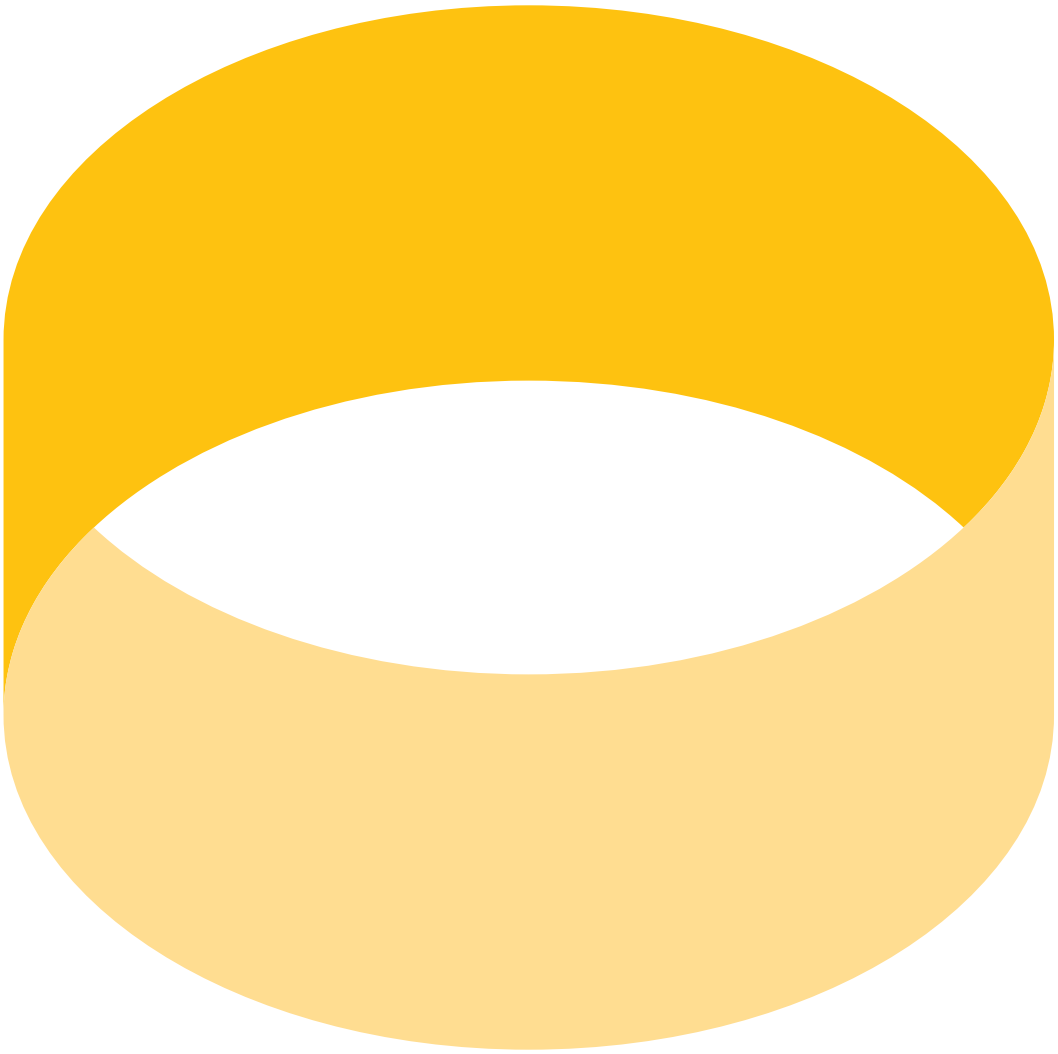


Uncovering Elusive Endpoint Threats

A two-phase approach to understanding your entire endpoint environment and reducing the risk of a breach

WHITE PAPER

Symantec™

The State of the Threat

The most dangerous and damaging threat is the one you don't see coming. Attackers know the best way to stay under the radar is not to use malware, but steal and use the credentials of legitimate users. Attackers are increasingly relying on these 'living off the land' tactics, making use of tools and credentials already installed on targeted endpoints to establish persistence. It helps them remain invisible and go about their business undetected. In fact, a recent Symantec study found that 94.5 percent of analyzed PowerShell scripts were malicious.

For example, with legitimate credentials, an attacker can elevate their access within the network to include operating system (OS) services, VPN communications, remote desktop proxies, and server configurations. They can operate in plain sight and carry out their attack activities on your endpoints without anyone seeing them. Or can they? Symantec Endpoint Detection and Response (EDR) Cloud can assess your endpoint environment and shine a light on these tactics to reveal attackers who have previously remained elusive in your environment.

EDR Cloud introduces a new approach to exposing and responding to breaches and unauthorized access, one that turns traditional detection and incident response methods upside down. This paper details this new approach and demonstrates the value it brings to your business' security.

Why Traditional Incident Response is Flawed

Despite the changing 'living off the land' tactics increasingly used by attackers, many organizations continue to rely on signature-based antivirus and known indicators of compromise (IOCs) to identify attacks. Unfortunately, these detection methods cannot detect new, unknown or zero day threats and are unable to identify stolen user accounts or lateral movement. What's needed is a way to uncover the unknown and undefined – the anomalous signs of a breach that aren't tied to malware.

Uncovering these 'signs' has typically fallen on the shoulders of the incident response (IR) team. They are the ones responsible for following up on an alert or a tip from law enforcement, a customer, or partner that something might be wrong. It is up to these highly skilled cyber analysts to figure out what is happening and, if an attack, resolve the impacts.

This can take days, weeks, even months, as the IR team collects and sifts through mountains of data investigating an incident, many of which end up being false alarms and a waste of time. For every digital artifact they find, there are more questions and manual investigations that need to be performed.

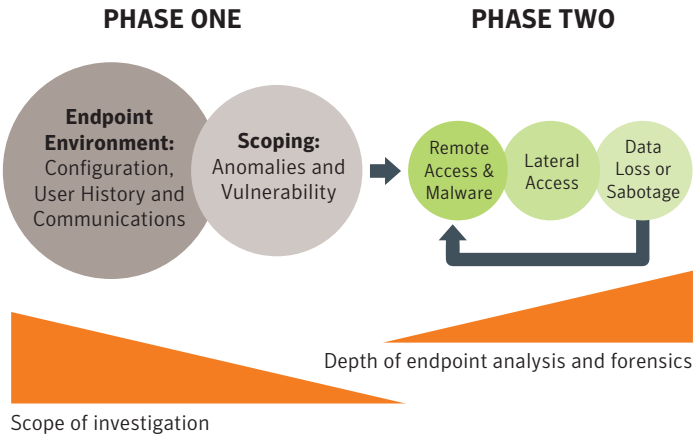
To completely remediate an attack, all links need to be revealed and all potentially impacted systems identified. Unfortunately, most of the time, the root cause and full attack timeline cannot be found, leaving the organization vulnerable to re-infection. It's like a whack-a-mole strategy – when one thing gets shut down, something else pops up.

What's needed is a way to see the full picture – to see how everything fits together, so that attack activity stands out and is fully understood. This is what EDR Cloud can do.

EDR Cloud Brings Clarity and Efficiency to IR

Rather than relying on a single IOC or source of threat intelligence, EDR Cloud looks at the whole picture from every angle. It uses automated security analytics to efficiently examine your endpoint environment as a whole. It dynamically baselines what is normal to make it easy to quickly identify software discrepancies, configuration anomalies and behavioral outliers that aren't normal or expected. This approach is effective at identifying unknown, zero-day threats because there are no preconceptions about what to look for and no need to have prior knowledge of trouble spots. It lets the actual activity (data) do the talking.

EDR Cloud uses a two-phase approach: Phase One takes a broad scope of the entire enterprise, while Phase Two takes a deeper dive into specific suspicious endpoints. Instead of performing time-consuming, traditional forensics of disk and memory images to try to spot attack activity, EDR Cloud automatically collects and normalizes the right forensics data needed to understand the full scope of what's happening.



Phase One: Environment Assessment

Phase One is a top-down examination of the environment, which ultimately narrows down the scope of what needs to be looked at more carefully to a manageable set of endpoints. During this phase, EDR Cloud collects and analyzes metadata from endpoints to understand usage patterns, statistical outliers, user behavior anomalies, and vulnerabilities. Unknown binaries are run through multiple analysis engines and the results are provided to your analysts, so they can quickly see where you have problems. This phase can identify:

- **Configuration Vulnerabilities**. The versions of commonly exploited client-side programs, such as Microsoft Office, Java, Adobe Acrobat, Active X, Media Player and Internet browsers, that contain unpatched or vulnerable software.
- **Browser Configurations**. Browsers with locally set proxy ports, browser extensions, plugins, and helper objects that are at greater risk or may have been exploited.
- **User Account Abuse**. User profiles and logon events that indicate potential account abuse, accounts that have cracked passwords, or pass-the-hash lateral movement behavior.
- **Persistence Mechanisms**. Registry, load order, tasks, startup programs, and other methods that enable software to persist on an endpoint, even after a rebootare examined to identify any threats and establish timestamp information as a starting point for future timeline analysis.
- **Memory and DLL Injection**. Loaded memory is examined to determine if programs have been injected into other programs, which is a common technique used by remote access tools and malware.
- **Command Line and Interactive Behavior**. Prefetch, superfetch, lnk, shellbags, MRU, registry entries, and file timestamps are used to locate suspicious program and user behavior.
- **AV Quarantine Logs**. AV logs are examined to help locate malware and previous infections.
- **Perimeter Event Logs**. Perimeter security device event logs are examined to help identify potential attacks, vulnerable machines, and previous infections.
- **DNS Logs**. DNS logs are examined to help identify at risk machines.
- **Customer Supplied Previous History**. Customer data is analyzed to help scope which machines and user profiles warrant further examination.

Phase Two: Deep Analysis and Threat Behavior Verification

Phase Two takes a closer look at high-risk endpoints identified in Phase One to validate threats and reveal the full extent of the incident's activity. Instead of the traditional, broad analysis of hard drive and RAM images, EDR Cloud surgically collects the relevant data and digital artifacts needed to validate an attack. These may include master file table records, event logs, registry hives, change journals, memory snapshots and other sources. The information is automatically normalized, organized and reconstructed into an attack timeline, so analysts can see the root cause and all the impacted components of the attack. In addition, this phase evaluates:

- **Additional Indicators**. Additional queries can be created to quickly and efficiently search the environment as a whole for other known indicators of threats.
- **Network Connections and IP Reputation**. Network connections from suspicious processes are compared against an IP reputation database.

- **Browser History**. The history of web browsing, both by users and programs that use Internet browser APIs, will be evaluated for suspicious behavior.
- **Software Usage History**. Event logs are examined to determine if any client-side software has crashed. Crash logs may also be used. This provides a starting point for timeline analysis and helps determine whether a machine has been exploited.
- **Memory Artifacts**. Memory snapshots of suspicious processes and modules are examined, including strings and possibly code, to determine if they is an malware or hacking tools.
- **File Artifacts**. Suspicious files, including those found in the timeline analysis, are pulled for examination.
- **File Behaviorals**. Certain executable files are evaluated in a sandbox to determine runtime behavior and identify malicious activity.
- **MFT, USN Change Journal, System Restore Points**. These digital artifacts contain a treasure trove of time-stamped endpoint behaviors that can be used for forensics timeline analysis.
- **Event Logs, Registry Hives**. These are additional digital artifacts that contain time-stamped endpoint behaviors that can be used for forensics timeline analysis.
- **Reverse Engineered Binaries**. Aside from automated binary analysis, analysts have easy access to download binary files to examine command and control loops, uncover internal functions and encryption methods.

EDR Cloud Delivers Results

With the endpoint visibility and analysis that EDR Cloud provides, IR analysts finally have what they need to quickly spot, understand and shut down the full extent of threats in your environment. No longer do you need to rely on costly, time-consuming manual IR processes to try to piece together what's happening in your environment – you have the root cause and timeline at your fingertips.

Arming your IR team with the right digital evidence and contextual information delivers exceptional results. You can:

- **Understand threats in your environment:** identifying all affected endpoints, uncovering lateral movement and user account propagation and documenting the technical details of the breach
- **Respond faster:** planning and executing an effective response that remediates all impacted components of the attack to ensure nothing persists.
- **Reduce risk:** making configuration changes, based on vulnerabilities identified in the environment, to improve your overall security stance, as well as establishing processes for continuous monitoring of the network that help you get ahead of threats.

EDR Cloud gives you the tools you need to efficiently identify and protect against the ever-evolving tactics attackers are using to target your organization, now and in the future.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, 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 and LifeLock product suites to protect their digital lives at home and across 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

SYMC_wp_Uncovering_Elusive_Endpoint_Threats_EN_v1e