

SECURITY AS A SERVICE



**FOR MORE INFORMATION
CONTACT US**



SECURITY AS A SERVICE



WHO WE ARE

Founded in 2009, SourcetekIT's Security as a Service team is dedicated to getting ahead of cyber threats before they can stop business. Our subject matter experts are sought-after authorities in IT security, risk mitigation, compliance, gap analyses and threat remediation, with decades of experience consulting, auditing, training and implementing enterprise security across multiple industries and for multiple resellers.

Our principal consultants literally wrote the book on compliance frameworks like NIST. They have trained thousands of CISSPs to be CISSPs, and authored books on the fundamentals of information systems security. As a result, we have contractual relations with more than 100 CISSPs who specialize in multiple market sectors, including healthcare (HIPAA/HITECH), retail (PCI-DSS), government contracting (ISO/NIST) & European markets (GDPR).



REAL-TIME AUTOMATED ENDPOINT SECURITY.

STARTED WITH DIFFERENT APPROACH TO ENDPOINT SECURITY

SourcetekIT was founded by cybersecurity professionals familiar with cyber warfare tactics designed to evade traditional endpoint security defenses. SourcetekIT mission is to deliver a comprehensive real-time endpoint protection offering post- and pre-infection protection against advance malware. SourcetekIT provides the only endpoint security solution offering correlated post and pre infection protection layers against advance.

POST-INFECTION PROTECTION

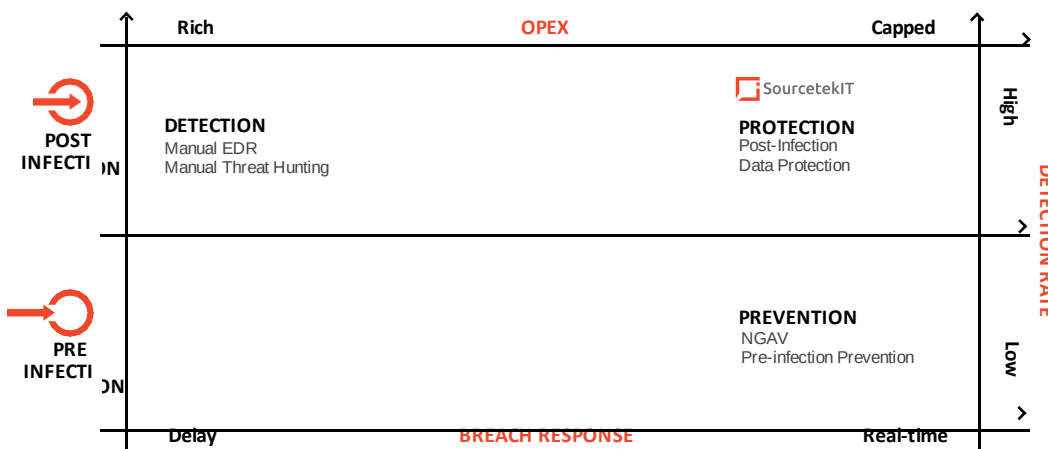
SourcetekIT is the only vendor that stops and contains advance malware from causing a breach impact in real-time after the endpoint has been infected as part of a multi-layered defense strategy. SourcetekIT eliminates dwell time and provides a suite of Endpoint Detection and Response (EDR) features to detect, contain, investigate and remediate.

PRE-INFECTION PROTECTION

SourcetekIT provides a first layer of defense custom built, kernel level Next Generation AntiVirus (NGAV) engine with machine learning features, to prevent infection from known and unknown malware.

SourcetekIT DIFFERENT APPROACH STOPS ADVANCE MALWARE, ELIMINATES BREACH RESPONSE GAP AND CURTAILS YOUR OPERATIONAL EXPENSES

Stop getting frustrated with legacy EDR and NGAV security software that has over-promised and under-delivered while driving up your costs. SourcetekIT caps operational expenses associated with post- and pre-infection endpoint protection management while delivering high detection rate with real-time response capabilities compared to traditional NGAV and EDR tools.



FEATURES

- ✓ **Detec^on** - Best user interface that eliminates alert fatigue
- ✓ **Containment** - First and only real-time post infection blocking of data exfiltration and tampering
- ✓ **Investiga^on** - First to eliminate dwell time and unify threat hunting, forensics, incident response and classification
- ✓ **Remedia^on** - Best virtual patch capabilities to preserve business continuity
- ✓ **Preven^on** - First and only kernel level NGAV with machine learning enrichment

BENEFITS

- ✓ **Protec^on** - Detect, block and stop the impact of malware
- ✓ **Management** - Complete console with intuitive interface
- ✓ **Scalability** - Lightweight agent of 20MB that can be deployed in minutes
- ✓ **Flexibility** - Support a broad range of operating systems
- ✓ **Cost** - Eliminate breach impact cost and operating expense



GIVES YOU BETTER PROTECTION, WITH AN INTUITIVE INTERFACE THAT IS MORE COST EFFECTIVE TO MANAGE AT SCALE



SourcetekIT PROVIDES A COMPREHENSIVE ENDPOINT SECURITY PLATFORM

SourcetekIT is the only endpoint security vendor built from the ground up to detect advance malware, contain and stop breach impact in real-time allowing you to investigate and remediate to preserve business continuity and prevent against known and unknown advance malware.

PRE-INFECTION	POST-INFECTION			
 PREVENTION Stop breach pre execution	 DETECTION No alert fatigue	 CONTAINMENT Stop breach post execution	 INVESTIGATION Full attack visibility	 REMEDIATION Disinfection
- Kernel level NGAV - Application Communication Control - Eliminate data tampering and exfiltration	- Provide malware classification - Display IOCs - Deliver full attack chain	- Real-Time post-infection blocking - Eliminate data tampering and exfiltration - No dwell time	- Conduct threat hunting on your time - Conduct incident response - Capture forensics data	- Virtual Patching: surgical removal of bad files and processes - Preserve business continuity - Connect to remediation tools via REST API

SourcetekIT SUPPORTED PLATFORMS



Windows XP SP2/SP3, 7, 8.x and 10.x, Windows Server 2003 R2, 2008 R2, 2012, 2012 R2, 2016, 2019



Yosemite (10.10), El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14)



VDI Environments: VMware Horizons 6 and Citrix XenDesktop/XenApp 7



Red Hat Enterprise Linux 6.8 and 7.x



CentOS 6.8 and 7.x



Ubuntu 18.04

“ SourcetekIT blocked malicious activity from spreading or corrupting the manufacturing line with malware and allowed the infected devices to continue manufacturing without any service interruptions.**”**



INTERNAL VULNERABILITY ASSESSMENT

PERFORMED TWICE A YEAR OR WHEN NEEDED

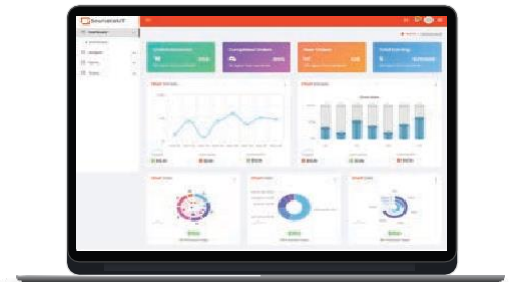
Identifies any open ports, vulnerabilities within the system. A report is made based on this assessment to allow for the creation of a mitigation plan.

WHAT DOES A VULNERABILITY ASSESSMENT DO?

Vulnerability Assessment is performed to discover any security risks in the system in order to prevent the likelihood of a threat. A vulnerability is any weakness the system has within its procedures, design, or any internal control that may be due to any violation of the system's security policy. This assessment allows for a mitigation process to be put into place to prevent intruders (hackers) from getting unauthorized access.

THE GOALS AND OBJECTIVE OF PERFORMING A VULNERABILITY ASSESSMENT

Based on the specific requirements from the client, SourcetekIT will accordingly set the rules of assessment and allocate the resources needed for the Vulnerability Assessment.



1. All required information will be gathered for the purpose of the assessment
 - Any information regarding the network inventory is to be collected
 - Access and or appropriate credentials required to gain entry into the network and its devices are to be obtained
2. Application is to be tested
 - Assessment experts will use the appropriate tools and software to discover the weaknesses within the system.
 - To uncover more complex findings manual penetration testing techniques can be used in the process.
3. Reporting
 - Analyze the data and information acquired from the assessment.
 - Document each stage of these findings.
 - Create a Report to be shared with the business to further formulate a mitigation plan.

EXTERNAL PEN TESTING

PERFORMED TWICE A YEAR OR WHEN NEEDED

Identifies vulnerabilities in the network and performs an external testing to understand how the system can be breached by an outsider, allowing for preventative measures to be put into place. This test is performed twice a year or when needed.

WHAT DOES PEN TESTING DO?

The primary objective of pen testing is to determine security weaknesses that could potentially be exploited by hackers. This test is performed by gathering the required information about the target,



determining the potential vulnerable endpoints, attempting a break into the system and then report these weaknesses. With the use of these findings system administrators are made aware of where the network is most vulnerable and how to plan to remediate.

WHAT DOES A PEN TEST REPORT INCLUDE?

Summary of Findings

The summary will document the results of the automatic security scan. Referencing all dates and time zones in which these scans are performed. When the scan started and ended at. It then talks about the order in which the content is outlined within the report. Also providing an overview on all the host IP's that have been scanned and also the severity of the type of vulnerability associated with each scan; high, medium or low.

Findings Per Host

This report will then further provide a detailed description on the findings of each host, stating the IP address, the threat level, summary of the discovery, the vulnerability detection result, the solution, and the references.

1. **IP Address:** The IP address that the scan is being done on is listed within the report. Having an IP associated with each detected vulnerability helps in narrowing down where the vulnerability is located within the network.
2. **Threat Level:** There is a threat level assigned to each detected vulnerability that is being scanned. This threat level is based on the severity of the vulnerability detected. Having a threat level assigned to each vulnerability will help system administrators prioritize threats during the mitigation process.
3. **Summary**
 - Vulnerabilities Detected
 - The impact it will have on the solution
 - The affected software
 - Insight on why this vulnerability may be caused
 - The method used to detect this vulnerability
 - References
4. **Vulnerability Detection Result:** The vulnerabilities that are detected during the scan will be identified, this can include details on any; open ports, software that isn't needed on the server, outdated software, patches that haven't been applied, SQL injection attacks, buffer overflows, cross-site scripting, capturing banners that identify the version of software on the server, least privilege violations etc..
5. **Solution Type:** Once the vulnerability type is detected, this report will also outline the mitigation process.
 - Explaining where the problem resides
 - If any change is to be made in the environment
 - What that change entails and the steps associated with it to remediate
6. **Vulnerability Detection Method:** Each step that was taken to map where the vulnerability is located will be outlined within the methodology of detection. This will detail the chain and areas that are insecure, potential algorithms that require change.
7. **References:** This section simply provides references used within this scan.

Recommendations

Each finding per host listed in this report provides steps of the remediation process for every separate vulnerability identified a part of the scan. The purpose of this report is to analyze what vulnerabilities are present. It is within the mitigation process where the system administrators can further make the changes to better secure their network.



DOMAIN PROTECTION SERVICE

Detects and stops any threats relating to; identity theft, spam accounts or any other compromises being made from the domain.



Send Spam from Compromised Email Account



Data Breach



Deface Web Properties & Host Malicious Content



Identity Theft



Compromise Other Accounts Using the same Credentials



Install Malware

Protect your credentials and stop unwanted access to your devices.

BACKUP ONE MAIN SERVER

Provides easy restoration of data and encrypts data storing it in the cloud. 1TB Backup is included anything above 1TB there will be an extra charge.

Our Backup and restore process is easy & Secure.

- Easy Restore
- Encrypted backup in the cloud
- Restore to VM for DR

Backup serves and company data in the secure encrypted cloud to avoid any Ransomware related issues. Backup your data to the external encrypted device, ask us how.

