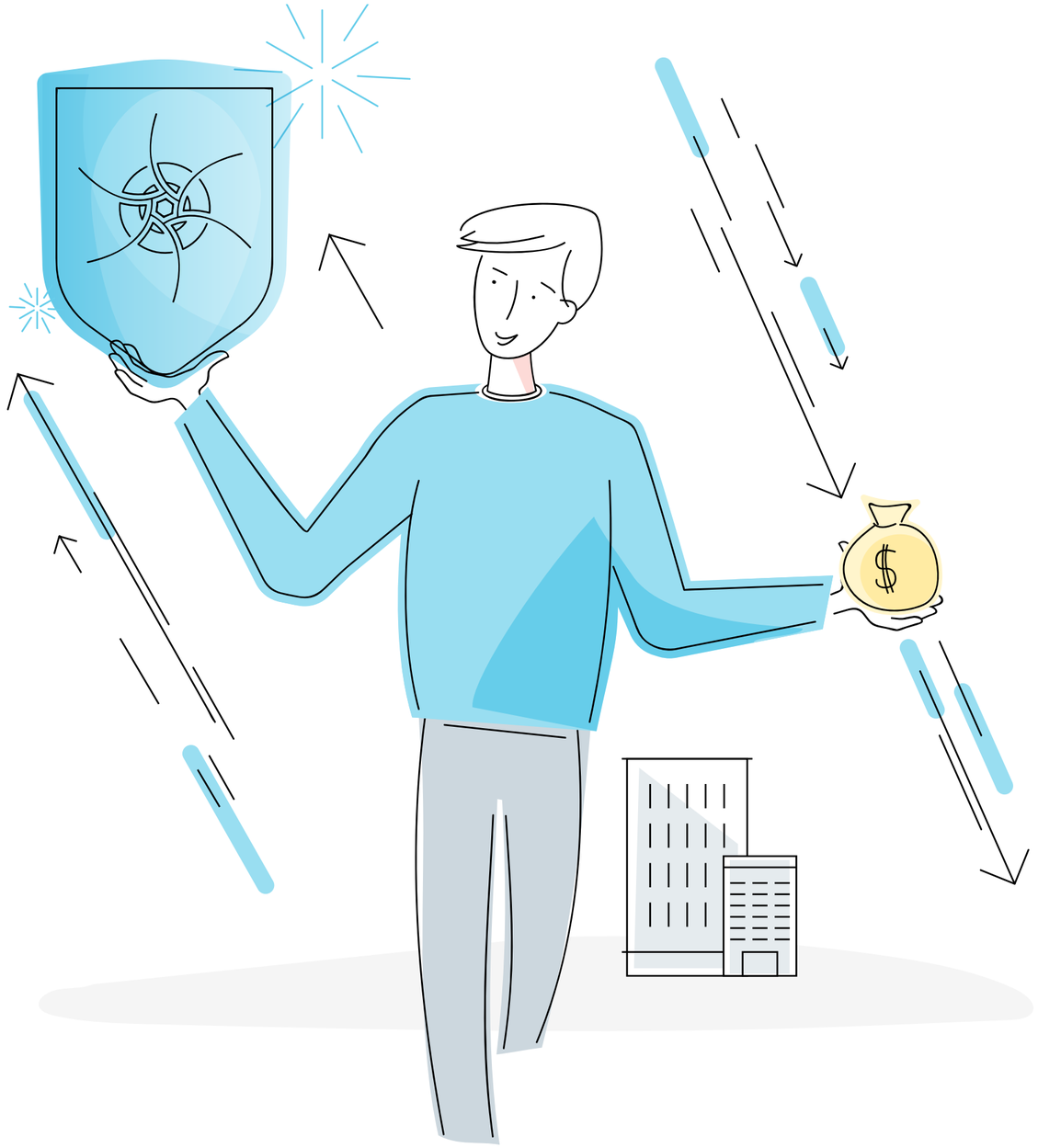
Cynet

SELF-AUDIT GUIDE

CYBER SECURITY EFFECTIVENESS FOR THE RESOURCE-CONSTRAINED ORGANIZATION

A Primer for Moving Beyond AV and Firewalls



AMERICAN TECHNOLOGY CLOUD, LLC

The Problem

As software systems become more distributed and interactive with cloud services tightly woven into organizations' architecture, defenders are left blind and impotent. Despite the endless parade of new security technologies - sandboxes, next gen firewalls, next generation antivirus, and so on - breaches continue as attackers bypass whatever the industry produces.

The bad guys continue to step-up their game. Just the growth of malware alone tells the story: The AV-TEST Institute registers over 250,000 new malicious programs every day.

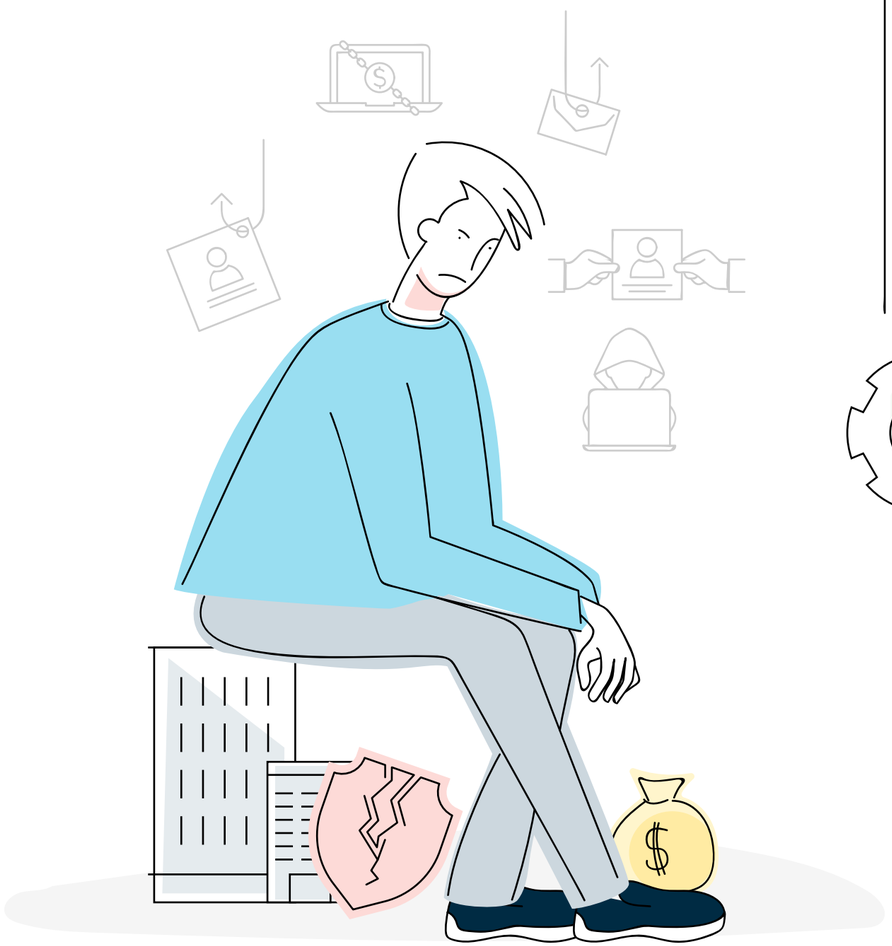
Eighty-two percent of malware disappears after one hour while just 70% of malware only exists once. It would take over 28-years just to detect the malware generated in a day.

Despite the billions in venture money that has poured into security startups, the majority of new vendors focus on larger enterprises with bigger budgets.

Today, big companies with million-dollar cyber budgets assemble a comprehensive cyber defense strategy, including dozens of security solutions to block and mitigate a wide variety of attacks such as phishing, ransomware, DDoS, APT and so on.

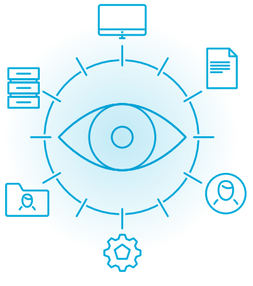
But what do you do if you're resource constrained, without the benefit of full security staff?

Regardless of size, basic disciplines exist that all companies should heed: The Fundamental Five.



THE SELF AUDIT CHECKLIST:

THE FUNDAMENTAL FIVE



VISIBILITY

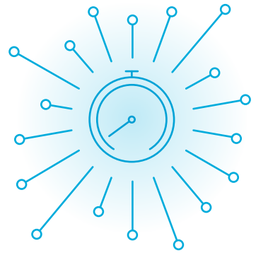
Know what you have to secure. And that means everything - you can't secure what you can't see. The basics include:

- Workstations and servers by operating system
- Installed software
- Configuration per asset company-wide
- Login visibility across the organization by date, time and location
- Folder shares: local and centralized

ASSET MANAGEMENT

Monitor and maintain the critical security components which you identified in step one. The basics include all details per asset including

- Users
- Applications
- Context-based network activity
- Performance details
- Certificates



PERFORMANCE

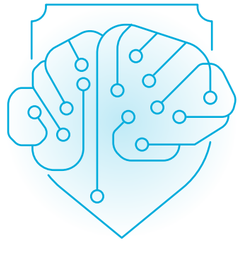
When an attack occurs, performance changes are certain. Checking system performance using some key criteria, is essential. The basics include:

- Total CPU percentage
- System partition size
- System partition free space
- Memory percentage
- Total memory
- Total free memory
- Number of connections
- Number of logged users

COMPLIANCE

Many, if not all, companies face regulation. To mollify regulators, organizations need to implement and report basic security activity. The basics include:

- Missing operating system patches
- Vulnerabilities
- Password age
- Allowed login
- Audit



EXPERTISE

Expertise in confirming exposures, closing simple issues, and escalation procedures. The basics include:

- 24/7 coverage against global, automated attacks
- Incident response
- Malware reverse engineering
- Threat hunting
- Forensics

What is Needed for an Effective Defense? The Way Forward

Effectively performing the Fundamental Five requires deploying many solutions (firewall, AV, SIEM, EDR, analytics, and more) operated by a security team with deep expertise. But for the resource-constrained organizations, this path is not viable due to high costs with few resources. Surveys show that resource constrained organizations rely mostly on firewalls (76%) and AV (81%)--but little else.

Ideally, these organizations should leverage an all-in-one security solution - an integrated platform that combines essential controls and correlates intelligence across them to deliver a robust defense.

ALL-IN-ONE SECURITY PLATFORM

Cynet makes cyber security simple. Cynet installs in less than two-hours for immediate coverage without any training. Once installed, Cynet simplifies ongoing management with precise and automated monitoring to complement your existing staff - even if you don't have any.

With a bird's-eye view across users, the network, files and endpoints, organizations gain unparalleled control and visibility to understand and mitigate threats.

Cynet simplifies cyber defense by converging essential security technologies and expertise.

Cynet's technical innovations converge endpoint protection, Endpoint Detection and Response, vulnerability management, deception, threat intelligence and network and end-user analytics.

In addition, Cynet's cyber SWAT team monitors all customer environments 24/7 and provides expertise for incident response, malware analysis, threat hunting and forensics.

Cynet is designed for organizations who want enterprise-grade security with complete protection for their network, without the heavy burden and overhead of deep cyber expertise.