



Cloud1 Solutions

# Cybersecurity Landscape

## Who is in your kitchen

### Overview


Learn about the real risk to the business and the active monitoring solutions available.

### Qualifying IT Outsourcing!


The attack surface has evolved pretty dramatically over the past few years, which can lead to blind spots across some of the most dynamic areas of your network, including cloud and container environments, as well as your web apps.

Avoid finding out months later that threat actors have been harvesting data that will be used to extort payment.

Luckily, tools exist today to eliminate these blind spots

 408 320 6966

 [info@cloud1solutions.com](mailto:info@cloud1solutions.com)

 [www.cloud1solutions.com](http://www.cloud1solutions.com)

Mike Wiechmann

## 1) 24/7/365 US based monitoring.



Adversaries don't work 9-5, nor do they adhere to a traditional Monday-Friday 40-hour work week. Business are under relentless assault 24/7 and so should your security team. A 24/7 SOC doesn't stop when business owners are asleep, but rather proactively hunt and monitor for threat indicators, even throughout holidays and weekends.

SOC monitoring around the clock keeps the threat radar circulating, hunting out advanced TTPs (tactic, techniques & procedures) to malicious hosts, networks and cloud artifacts - before a breach occurs.

## 2) Microsoft 365 email threat monitoring

One of the largest blindspots in the industry is the lack of visibility into Microsoft 365 user threat data and to constantly have eyes monitoring it. Our SOC platform purposely built for cyber industry, provides a artificial intelligence platform backed by seasoned security analysts hunting malicious and suspicious activity.

## 3) Sophisticated Security Scams

Education and training can help users spot scam emails. But they'll always miss some — and that's especially true for well-disguised BEC scams. Technology can provide multiple layers of additional security that rise to the occasion when frontline efforts fail

- a) Multifactor authentication
- b) Conditional policies
- c) 24/7 monitoring

## 4) Firewall and workstation thread detection

Firewall log analysis tool for security event management that collects, analyses, and reports on enterprise-wide firewalls, proxy servers, and VPNs to measure bandwidth usage, manage user/employee internet access, audit traffic, detect network security holes, and improve incident response.

## 5) Are you currently confident in your cybersecurity

While no longer overlooked at the same level it was years ago, cybersecurity is an essential part of your technology strategy. This is not a fair burden to put on your internal IT department, as they do not have the bandwidth or qualifications to outline your security posture. Furthermore, having someone inexperienced in cybersecurity leaves your business vulnerable to the many forms of cyber threats that exist today. Using a managed services provider can often mean improving your security posture as well, if the MSP has a team dedicated solely to your cybersecurity, and a virtual chief security officer to create a strong cybersecurity posture for your organization.

*“Outstanding! Already there is a clear and profound difference over what they have received in the past. Thank you so much!”*

-Leading Logistics Firm

### How we can help

Our IT team of experts can expand your capabilities, detect and respond to incidents and remediate.

Building your cybersecurity posture will help avoid exposure and downtime due to ransomware.



Cloud1 Solutions