blackpoint

Why Your Hybrid Workplace Needs a SOC

Good help is hard to find.
Especially when it comes to protecting cloud and hybrid environments.

With the cloud expanding the attack surface, threats in a hybrid environment can be difficult to detect and contain. The cybersecurity talent gap doesn't make this any easier. Over half of IT and cybersecurity leaders struggle to recruit and retain talent, and 68% of leaders agree that the cybersecurity skills shortage creates additional cyber-risks for the organization. The most difficult skill to find? **Cloud security expertise.**[1]

A SOC at your service

A security operations center (SOC) is staffed with experts responsible for monitoring, detecting, responding to, and mitigating cybersecurity threats and incidents. In-house SOCs are expensive to maintain, but no business should be left without coverage.

That's why using a managed SOC service is a smart move in our world of complex threats. A managed SOC team watches over hundreds or thousands of businesses, stopping attacks daily for customers of all sizes. With constant exposure to attacks of varying complexities and methods, a SOC-as-a-service team has developed an elite level of defense.

Typical organization's security team versus our elite SOC service

INTERNAL SOC TEAM

90%

of organizations say they are unable to detect, contain, and resolve threats within an hour.[2]

BLACKPOINT SOC

19 minutes

Average time to resolve escalated tickets.

Top 5 cloud attacks and how we pivot

Our SOC team has seen attacks on cloud and hybrid environments increase substantially in the recent past. Here are the most common ways we are seeing attackers exploit the cloud:

1. Bypassing multifactor authentication
2. Setting up rules that cause certain internal emails to forward to attacker-controlled account (post-exploitation)
3. Logging in from VPN or proxy to bypass geo-blocking, which blocks traffic from specific regions
4. Attacking applications that use outdated methods for authentication
5. Logging in from suspicious user agents—agents other than the usual web browser

As we see attack types rise in prominence, we fine-tune our detection systems, enabling us to better respond to that attack. For example, we recently updated our technology to immediately detect suspicious email forwarding rules, as well as instances of what we call impossible travel—bouncing between time zones or countries.

**Impossible travel is available with an upgraded Microsoft license.*

8 Reasons to Use a Managed SOC Service

EXPERTISE

Access to cybersecurity specialists with advanced skills and knowledge.

24/7 MONITORING

Continuous threat detection and response, even outside business hours.

COST-EFFECTIVE

Eliminate the upfront expenses of building an in-house SOC.

ADVANCED TOOLS

Benefit from cutting-edge security technologies for enhanced protection.

INCIDENT RESPONSE

Rapid, efficient response actions to contain and mitigate threats.

COMPLIANCE

Helps meet requirements with monitoring, response, and reporting capabilities.

REDUCED HIRING BURDEN

Avoid the challenges of recruiting and training cybersecurity staff.

SCALABILITY

Easily adjust protection levels as business grows and requirements change.

It's powerful to have an elite level of expertise and efficiency watching over your environment. And it's within your reach.

Blackpoint's SOC detects breaches in your and your customers' environments—and rapidly responds to contain them. We leverage proprietary MDR technology combining network visualization, insider threat monitoring, anti-malware, traffic analysis, and endpoint security into an end-to-end cyber solution protecting you and your clients.

Contact us today to find out how to get started with our SOC team at your service.

CONTACT US

[1] 2023 Cybersecurity Skills Gap report, Fortinet

[2] The State of Cloud-Native Security 2023, Palo Alto Networks