5 Signs Your Organization Lacks Cyber Visibility

Strengthen Your Defense with 24/7 Threat Monitoring and Incident Response

Why cyber visibility matters

In today's hyperconnected world, organizations are under constant threat from increasingly sophisticated cyberattacks. From ransomware to insider threats, these risks target every layer of the IT infrastructure, including networks, endpoints, cloud services, and user access points.

One of the most significant security challenges enterprises face is the lack of comprehensive cyber visibility. Without full visibility into network activity, user behavior, and system vulnerabilities, security teams operate in the dark—unable to detect, analyze, or respond to threats effectively.

C1's 24/7 Threat Monitoring and Incident Response delivers real-time visibility and protection across your entire IT environment. This proactive approach detects threats before they escalate, enabling swift action and reducing the risk of costly breaches.

Use this checklist to assess your organization's cybersecurity visibility and discover how C1 can close critical security gaps.

□ Sign 1: Limited awareness of network activity

What to look for

- Incomplete monitoring of on-premises, cloud, and hybrid network traffic.
- Siloed security tools that lack centralized visibility.
- Infrequent analysis of network logs and event data.

Why it's a problem

A lack of network visibility creates blind spots where malicious activity can go undetected. Cybercriminals exploit these gaps to move laterally within the network, escalate privileges, and exfiltrate sensitive data without being noticed.

Many organizations rely on disjointed tools that generate massive amounts of uncorrelated data, overwhelming IT teams and delaying threat detection.

The risk

- Increased susceptibility to advanced persistent threats (APTs) and ransomware.
- Delayed detection of insider threats and unauthorized access.
- Higher chances of prolonged breaches and data exfiltration.

How C1 helps

- C1 SOCaaS (Security Operations Center as a Service) delivers 24/7 centralized network monitoring, offering real-time visibility into all network traffic.
- Integration with Cisco Secure Firewall and Cisco SecureX ensures continuous analysis of security events for faster detection and response.
- Automated workflows prioritize alerts and streamline investigations, eliminating blind spots.

□ Sign 2: Inability to detect insider threats

What to look for

- Limited monitoring of employee activities and privileged access.
- No identity and access management (IAM) policies in place.
- Lack of behavioral analytics to detect unusual user actions.

Why it's a problem

Insider threats are among the most difficult to detect because they often involve trusted users misusing legitimate access.

Whether malicious or accidental, these actions can lead to significant data breaches, compliance violations, and reputational damage.

The risk

- Sensitive data exposure through unauthorized access or negligence.
- Intellectual property theft or data leaks.
- Difficulty identifying compromised employee accounts used for attacks.

How C1 helps

- Cisco Duo Security enforces strong access controls through multi-factor authentication (MFA) and Zero Trust security principles.
- C1 Managed Detection & Response (MDR) continuously monitors user behavior to detect anomalies and prevent insider threats.
- Identity and privilege management policies are integrated to reduce access misuse.

□ Sign 3: Gaps in endpoint monitoring

What to look for

- Inconsistent endpoint security coverage, especially for remote and hybrid users.
- Outdated antivirus or antimalware solutions with no real-time threat detection.
- No centralized management of devices and security policies.

Why it's a problem

Endpoints are often the first point of entry for cybercriminals, especially in hybrid work environments. Laptops, mobile devices, and unmanaged endpoints introduce significant vulnerabilities if not continuously monitored and protected.

The risk

- Malware and ransomware infections via unprotected devices.
- Unauthorized access to corporate networks through vulnerable endpoints.
- Loss of sensitive data through compromised or stolen devices.

How C1 helps

- Cisco Secure Endpoint provides advanced malware protection, real-time monitoring, and response across all devices.
- C1 SOCaaS integrates endpoint detection and response (EDR) into a unified security strategy.
- Automated patch management and vulnerability scans ensure endpoints are always protected.

□ Sign 4: Delayed threat detection and response

What to look for

- Long response times to security alerts due to manual analysis.
- Overwhelmed security teams unable to manage high volumes of security data.
- Inconsistent incident response procedures across teams.

Why it's a problem

Speed is critical when responding to cyber threats. Delayed detection and slow response times can allow attackers to escalate privileges, exfiltrate data, or launch damaging attacks.

Manual processes and alert fatigue often overwhelm IT teams, causing critical alerts to be missed or ignored.

The risk

- Increased breach severity and longer recovery times.
- Higher financial losses due to ransomware or data theft.
- Damage to brand reputation and customer trust.

How C1 helps

- AI-powered threat detection through Cisco SecureX and Talos Intelligence accelerates detection and response.
- C1 SOCaaS automates incident response workflows to reduce response time.
- Customized playbooks ensure consistent, efficient handling of security incidents.

□ Sign 5: Lack of visibility into cloud and SaaS environments

What to look for

- Limited security controls for cloud services and SaaS applications.
- No centralized visibility across multi-cloud environments.
- Inadequate monitoring of cloud workload security configurations.

Why it's a problem

As organizations adopt hybrid and multi-cloud strategies, the lack of visibility into these environments leaves them exposed to misconfigurations, unauthorized access, and cloud-based attacks.

The risk

- Cloud misconfigurations leading to data exposure.
- Unsecured SaaS applications creating entry points for attackers.
- Compliance violations due to lack of visibility into cloud security.

How C1 helps

- Cisco Umbrella provides DNS-layer security and threat protection for cloud applications.
- Cisco Cloudlock secures SaaS platforms, protecting data and user access.
- C1 Managed Services ensure continuous monitoring of cloud workloads and proactive risk mitigation.

How did your organization score?

- **0-1 signs:** Excellent visibility—maintain proactive security practices.
- **2-3 signs:** Moderate risk—consider expanding monitoring and detection capabilities.
- **4-5 signs:** High risk—immediate action is needed to improve cyber visibility.

Take action with C1 24/7 Threat Monitoring and Incident Response

Don't wait for a breach to reveal your security gaps. Get started today!

C1's 24/7 Threat Monitoring and Incident Response provides continuous protection, enabling your organization to detect and mitigate threats in real-time.

Contact a C1 Security Expert for a free consultation.

REQUEST A CONSULTATION

C1, the global technology solutions provider, transforms businesses by creating connected experiences that shape the future. With more than 6,000 customers, C1 empowers industries through secure, innovative technologies, collaborating with leading partners to deliver total lifecycle solutions. Learn more at onec1.com.