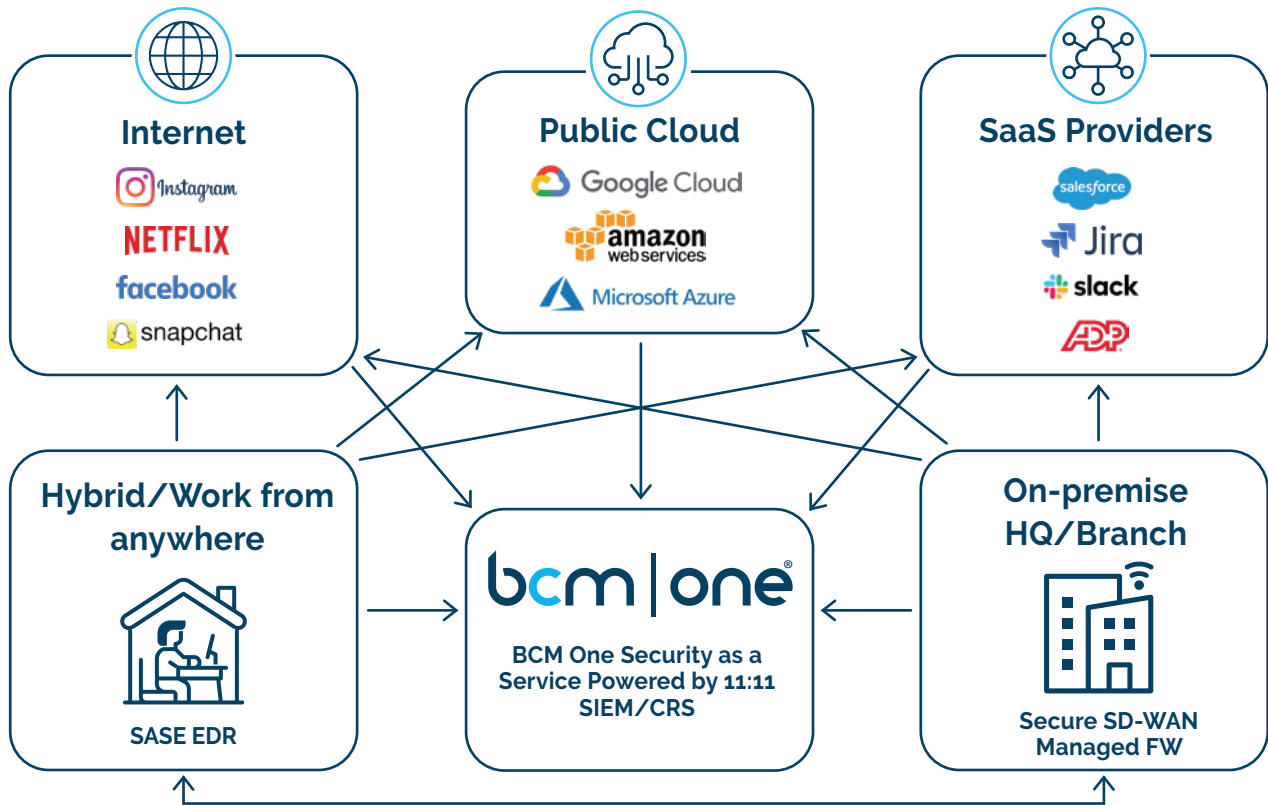# Managed Security Services

Cybercriminals could strike at any time —and they only need to beat your defenses once.

Security is a crucial concern for every business, and we see daily escalating reports of security incidents. With the increasing complexity of traditional and multi-cloud infrastructures and the high sophistication of today's cybercriminals, the need for dedicated security professionals who are highly trained and constantly focused is vital to ensuring proper protection of business-critical data—and it requires a multi-layered approach. BCM One delivers this with security incorporated across all of your on-premises, cloud-based, and endpoint resources.

Internet
Instagram
NETFLIX
facebook
snapchat

Public Cloud
Google Cloud
amazon web services
Microsoft Azure

SaaS Providers
salesforce
Jira
slack
ADP

Hybrid/Work from anywhere
SASE EDR

bcm|one®
BCM One Security as a Service Powered by 11:11 SIEM/CRS

On-premise HQ/Branch
Secure SD-WAN Managed FW

BCM One Incoming Network & Security Data

BCM One Egress Network & Security Data

=

Managed Network Services

- Monitor Notify and Restore
- VitalView
- SD-WAN Director
- Secure Access Service Edge (SASE)
- Data Leak Protection (DLP)
- Cloud Access Security Broker (CASB)
- Zero Trust Network Access (ZTNA)
- Secure Web Gateway (SWG)
- User and Entity Behavior Analytics (UEBA)
- Remote Browser Isolation (RBI)
- Intrusion Dedection/Prevention System (IDS/IPS)
- AV/Malware Protection (Inline AV)

+

Managed Security Services

- Continuous Risk Scanning (CRS)
- Managed Firewall w/Security Telemitry
- Security Information and Event Management (SIEM)
- Endpoint Detection & Remediation (EDR)
- Log and Alert Aggregation
- AI + ML Event Analysis
- Dedicated Security SOC Tier II Analysts

Managed secure SD-WAN and SASE

Application access with unparalleled reliability and security

BCM One's managed secure SD-WAN service allows you to rapidly, reliably, and securely access applications in the cloud and securely transmit voice, video, and data uninterrupted. And secure access service edge (SASE) provides a security layer on top of secure SD-WAN, enabling your remote workforce to securely access the company network using their preferred devices.


Key features

VitalView™
Cloud-based, geo-redundant platform providing 24/7/365 proactive monitoring, alerting, and restoration across all services, devices, and providers

SD-WAN Director
Native Versa Director access to see, customize, and run analytics and reports

Secure access service edge (SASE)
Endpoint network and security client to simplify IT infrastructure, improve threat detection and data protection, and reduce costs

Data leak prevention (DLP)
Prevent loss or leakage of sensitive information to protect intellectual property or for regulatory compliance

Cloud access security broker (CASB)
Placed between end users and cloud service providers to combine and interject enterprise security policies

Zero-trust network access (ZTNA)
Ensures access is granted on a need-to-know, least-privileged basis defined by granular policies

Secure web gateway (SWG)
Protects users and devices from Internet threats and enforces corporate security policies

User and entity behavior analysis (UEBA)
Detects anomalistic behavior for investigation of possible security events such as malware

Remote browser isolation (RBI)
Neutralizes online threats by hosting users' web browsing sessions on a gateway device instead of their endpoint devices

Intrusion detection/ prevention system (IDS/IPS)
Identifies possible incidents, logs details about them, stops them, and reports them to the orchestrator

AV/malware protection (inline AV)
Complements AV on endpoint machines to provide stream-based protection against malware

Security as a Service powered by 11:11

Stay ahead of internal and external threats with 24/7/365 managed security services

Our Security as a Service powered by 11:11 solutions protect your network from attackers, detect active malicious activities on endpoints, and identify risks across your managed infrastructure environments. With decades of cybersecurity experience, rely on our 24/7/365 Security Operations Center (SOC) to protect your infrastructure from malicious cyberattacks.
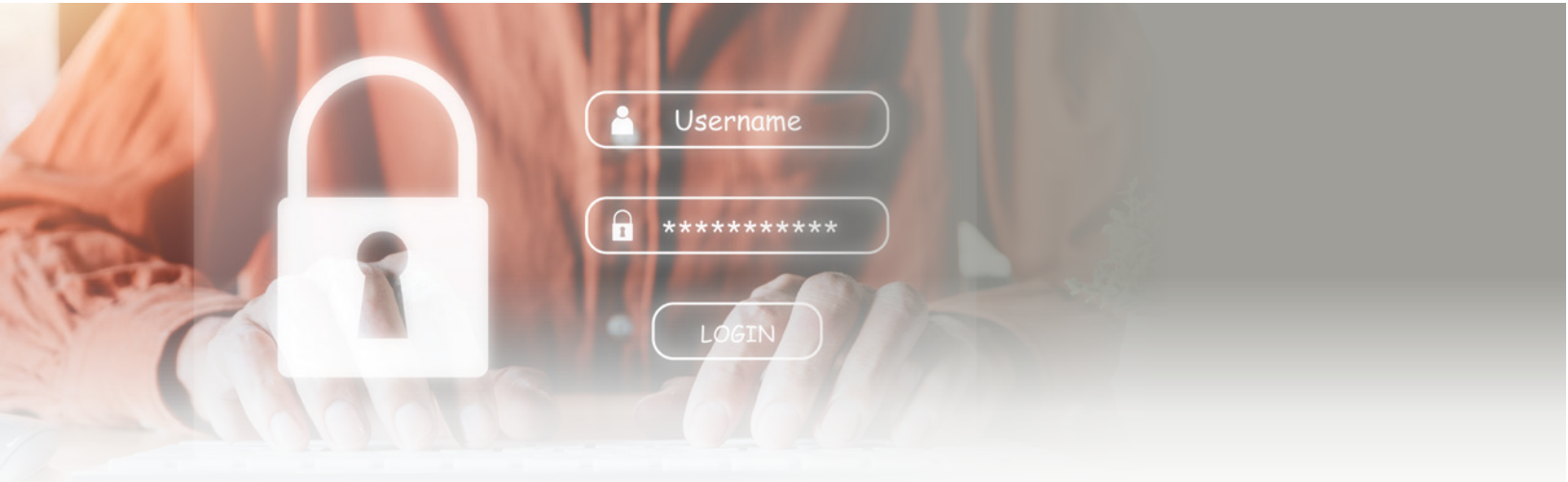
Security as a Service solutions

Managed Firewall

Immediately gain greater visibility into your network to help increase performance and guard against attacks and unplanned downtime. Built on the industry-leading Fortinet FortiGate next-generation firewall platform, and backed by an experienced SOC, you can rest assured that your network, employees, and data are protected.

Managed Security Information and Event Management (SIEM)

Identifying threats through log analysis often means detecting one log out of millions produced daily that could be harmful or malicious. While some security solutions monitor certain systems or applications, SIEM solutions provide visibility across heterogeneous and distributed infrastructure components and endpoints for real-time monitoring to reduce the mean time to respond (MTTR).

Continuous Risk Scanning

Tracking vulnerabilities, as part of an organization's security strategy is critical to identifying, remediating, and reporting on security vulnerabilities in systems and networks. Get deep, contextual risk analysis to prioritize vulnerabilities for remediation to minimize your attack surface.

Managed Endpoint Detect and Recovery (EDR)

The rapid growth of disruptive cyberattacks and highly distributed workforces has organizations reconsidering the tools they use to identify and respond to threats on their networks. Managed EDR enables you to get ahead of cybercrime, like ransomware, by reducing the time between detection and response. This improves your security posture by preventing and detecting threats on endpoints, and it minimizes the impact of incidents.

Contact us to get started today

bcm|one®

7/2023