

# Infinigate SOC as a Service

Infinigate Security Operations Center (SOC) as a Service gives your customers a 24x7 view of cybersecurity threats across their distributed endpoints. Not only that, but our in-depth analytics of threat data allows you to take rapid action to protect your customers' critical apps and data. With SOC as a Service, you can participate fully in the growing cybersecurity market, increase your services revenues, and build stronger, longer-lasting customer relationships.



Around the world, organisations and individuals are targeted with more than 2,000 cyberattacks every day – roughly one every 40 seconds. As well as causing disruption and distress, cyberattacks also have a major financial impact, costing up to 6,000 billion dollars a year globally.

To protect their critical applications and data, organisations need solutions that can protect them against all manner of cyberattacks, 24 hours a day, 365 days a year.

With Infinigate, you can provide a comprehensive Security Operations Center (SOC) as a Service for your customers. This provides 24-hour monitoring for their IT environments, giving them peace of mind that their endpoints and data are protected at all times, and supporting faster responses in the event of a suspected security breach.

Critically, our SOC as a Service offering allows you to participate fully in the fast-growing cybersecurity market and to grow your revenues accordingly. Equally importantly, it helps you increase the value you deliver for your customers vs. piecemeal security solutions, and helps you build long-lasting, trust-based relationships with them for repeat revenues year after year.

## What is Infinigate SOC as a Service?

Infinigate SOC as a Service is delivered via a cloud-hosted platform that sources and processes a range of data from customer endpoints to prevent and detect cyberattacks. With activity monitored constantly on each endpoint, the system collects large volumes of events and attributes from each endpoint and uses AI algorithms to process the data, spot potential security threats, and report on the security of each device on the network.

You and your customers can choose the security coverage you need from the following three solution 'tiers':

### Tier 1

#### **Threat detection and monitoring (24x7)**

This opens tickets for each suspected security breach related to a customer endpoint, and closes false positives to reduce manual interventions and workloads.

This also includes basic investigation of suspected security incidents and automated actions to mitigate potential risks. Threat detection notifications are delivered 24 hours a day, support is available from 9x5, and threat data is retained by the system for 365 days for forensic analysis. Monthly threat reports are also included.

### Tier 2

#### **Threat investigation and mitigation (9x5)**

This applies Cyber Threat Intelligence (CTI) to support proactive 'hunting' of potential security threats, helping organisations to discover new and emerging cybersecurity threats, or to understand where previously unidentified malicious actors are impacting their operations. Within tier 2, Infinigate makes recommendations of how threats can be successfully mitigated, allowing you to take fast action to protect your customers systems and data.

### Tier 3+

#### **Forensic threat investigation and reporting (9x5)**

Tier 3 of our SOC as a Service offering gives your customers access to the Infinigate Cybersecurity Incident Response Team (CSIRT), who will investigate potential breaches and take the actions required to restore security to endpoints or sets of endpoints. This tier of the solution also incorporates monthly reporting on detected security threats and associated actions for forensic analysis, and to inform actions that deliver continual security improvement for cybersecurity provision.

## The unique value of Infinigate's SOC as a Service

The Infinigate SOC as a Service combines our deep cybersecurity industry knowledge with our full featured analytics platform and support from our expert security teams. The solution also collects far richer event and attribute information from endpoints than competing solutions, providing a complete and forensic view of threats and supporting effective actions to mitigate them on an ongoing basis.

Infinigate's close relationships with the leading cybersecurity solution providers means that we configure and manage our solutions in an optimal way, ensuring that your customers' endpoints are constantly protected. We can also access direct vendor support when needed to mitigate and neutralise cybersecurity threats.

Our estate of endpoints under management is expanding by thousands of devices each year, and we are now recognised in the industry as one of Europe's leading providers of cybersecurity managed services. This means you can trust us to deliver mission-critical cybersecurity threat detection and prevention services for your clients, while also benefitting from the new revenue opportunities this service presents.



### Find out more

To discover more about Infinigate's SOC as a Service offering, and how it can help you maximise your cybersecurity revenues and increase value for your customers, please contact [servicesplus@infinigate.com](mailto:servicesplus@infinigate.com).

You can also find additional Infinigate professional IT services that help you maximise your revenues at [www.infinigate.com](http://www.infinigate.com)

### About Infinigate

Infinigate is an EMEA cybersecurity powerhouse covering over 100 countries. Our focus and deep technical expertise in cybersecurity, secure networks and secure cloud for SMB and enterprise set us apart. Our 1,250 employees provide locally tailored services complementing a robust central supply chain, sparking growth for our partners, MSSPs and vendors.