

# Security Device Management

Ensure your network infrastructure functions as designed, continuously, efficiently, and always up to date

## Security basics are still security basics

To protect your network systems, you have to be constantly vigilant against security threats. Simply deploying security devices isn't enough. Security devices such as IDS/IPS, FIMs, SIEMs, UTMs, VPNs, WAFs, firewalls and endpoint security solutions must be properly updated and patched to protect against internal and external threats. Policies, signatures and rules need to be updated and maintained to ensure accessibility, provide security and to comply with regulations.

Device Management is a challenge, but it doesn't have to be

BAE Systems' Security Operations Center (SOC) staff have specialized training in each technology that we support and act as an extension of your internal team to ensure the security devices which protect you, your business and your reputation are all switched on, working, up-to-date, correctly configured and functioning correctly, safeguarding your network 24/7, every day. All security events are processed and correlated by BAE Systems SIEM, which enables identification of threats that bypass perimeter devices. Security Device Management from BAE Systems consists of a range of services aligned to meet your desired outcomes, including:

- 24x7 event monitoring and alerting
- Ensure devices are configured according to manufacturers' guidelines
- Performance and availability management
- Device upgrades and patch management
- Real-time health monitoring
- Continuously manage and maintain devices
- Ensure vulnerabilities are identified and patched
- Keep devices up to date with relevant software upgrades
- Keep backups of configurations.

BAE Systems' allows your staff to better focus resources where they are needed, while ensuring that the infrastructure you have chosen to build around and within your network will function as you have designed it to, continuously, efficiently, and always up-to-date.

## Security Device Management Outcomes

SOC analysts manage and monitor device with a focus on rapid threat detection and full packet capture. Analysts look into the signature tripped, and then perform packet analysis to close the event.

SOC analysts focus on correlation of UTM events and applying threat intelligence to events. Analysts provide a deeper written analysis of events and contact customers directly for each incident. Many customers in highly regulated industries, which generally have higher security demands, utilize this option.

SOC analysts incorporate threat intelligence and track the activities and infrastructure of the groups responsible for the world's most sophisticated cyber attacks to block these attacks at the perimeter of your network.

BAE Systems' allows your staff to better focus resources where they are needed...

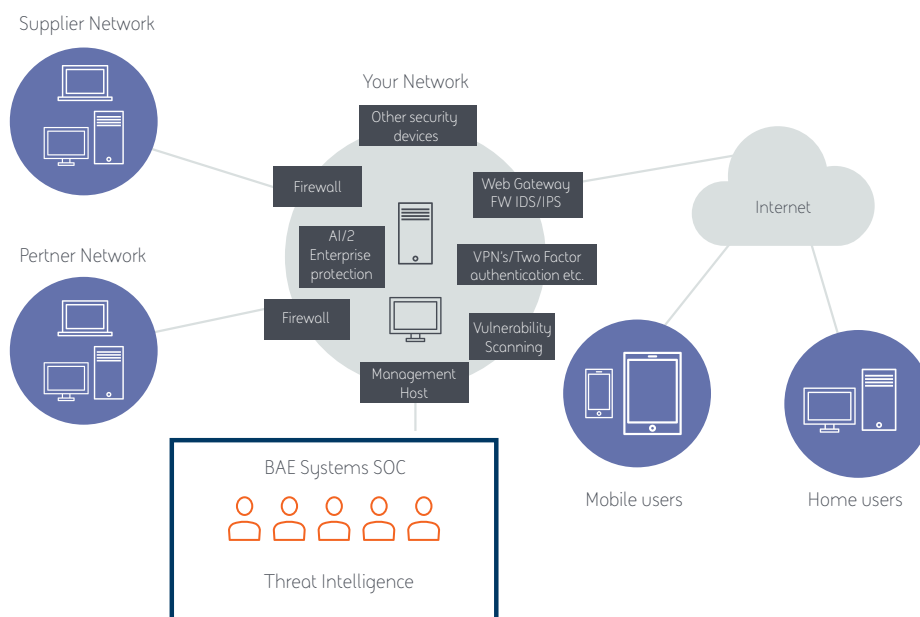
## Actionable Intel and Neighborhood Watch Effect

As part of the Security Device Management service you will benefit from our vast experience of global security threats: threats detected within our extensive client base or through our own threat intelligence will be blocked on your network through signature/blacklist updates.

## Benefits

- Improve operational efficiency
- Reduce redundant security technology investment
- Better protection coverage with correctly configured and optimized security equipment
- Reduce unnecessary cost and time mapping and archiving logs to meet data privacy and compliance auditing.
- Release constrained security staff to concentrate on more strategic efforts

## Security Device Management



## We Are BAE Systems

We help nations, governments and businesses around the world defend themselves against cyber crime, reduce their risk in the connected world, comply with regulation, and transform their operations. We do this using our unique set of solutions, systems, experience and processes - often collecting and analyzing huge volumes of data. These, combined with our cyber special forces - some of the most skilled people in the world, enable us to defend against cyber attacks, fraud and financial crime, enable intelligence-led policing and solve complex data problems.

BAE Systems, 265 Franklin Street, Boston, MA 02110, USA

T: +1 (617) 737 4170

E: [learn@baesystems.com](mailto:learn@baesystems.com) | W: [baesystems.com/businessdefense](http://baesystems.com/businessdefense)

 [linkedin.com/company/baesystemsai](https://www.linkedin.com/company/baesystemsai)

 [twitter.com/baesystems\\_ai](https://twitter.com/baesystems_ai)