SONICWALL®

SonicWall NDR SIEM / SOCaas

The Challenge is Expanding

- Cyberattacks and breaches are increasing
- Environments are more complex
- Security budgets are growing in response

Traditional Methods Can't Keep Up

One solution to this problem is to cobble together disparate solutions. But this leaves blind spots and creates a large amount of alert noise. This is why you see "prepared" organizations get breached.

Worse, it takes the industry an average of 200 days to detect a breach -- giving criminals more than six months to exfiltrate data! Clearly a better way of detecting, alerting and remediating these threats is needed.

Our Solution

Rather than ignoring blind spots, SonicWall's SIEM solution (backed by our 24/7 SOC) provides protection and centralized visibility for greater control over your security.

- Reduce breach detection to minutes
- Mitigate the risk of data exfiltration
- Improve the accuracy of security event detection
- Automatically piece together complex attacks across cloud, endpoint, network, user and applications
- Relax, knowing that you're keeping your clients safe

Discover what true partnership with a security provider is like: Increase visibility across your ecosystem and access rapid response from our fully manned 24x7x365 SOC.

To learn about the wide range of benefits enjoyed by SonicWall SecureFirst partners, contact us today!

partnerdevelopment@sonicwall.com

Powered by open extended detection and response (Open XDR)

Intelligent next- gen security operations platform
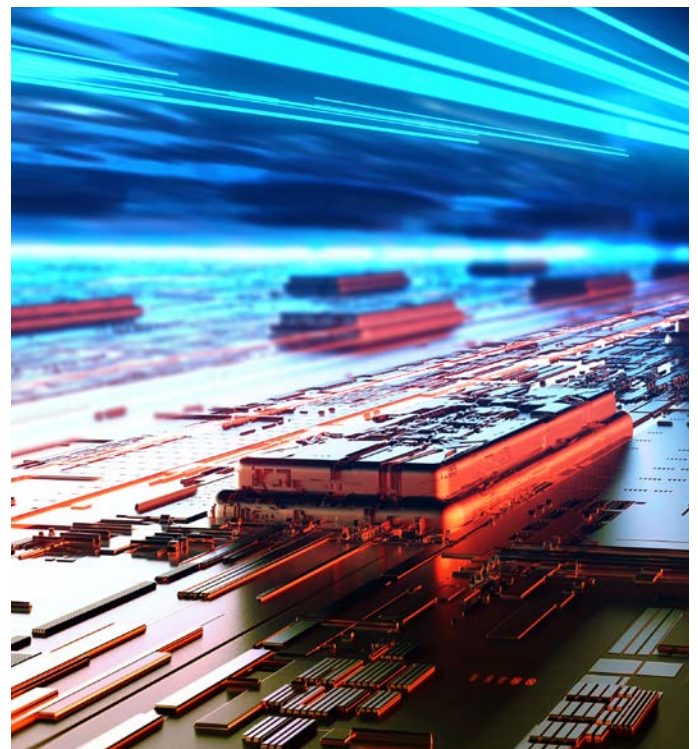
Artificial intelligence and machine learning
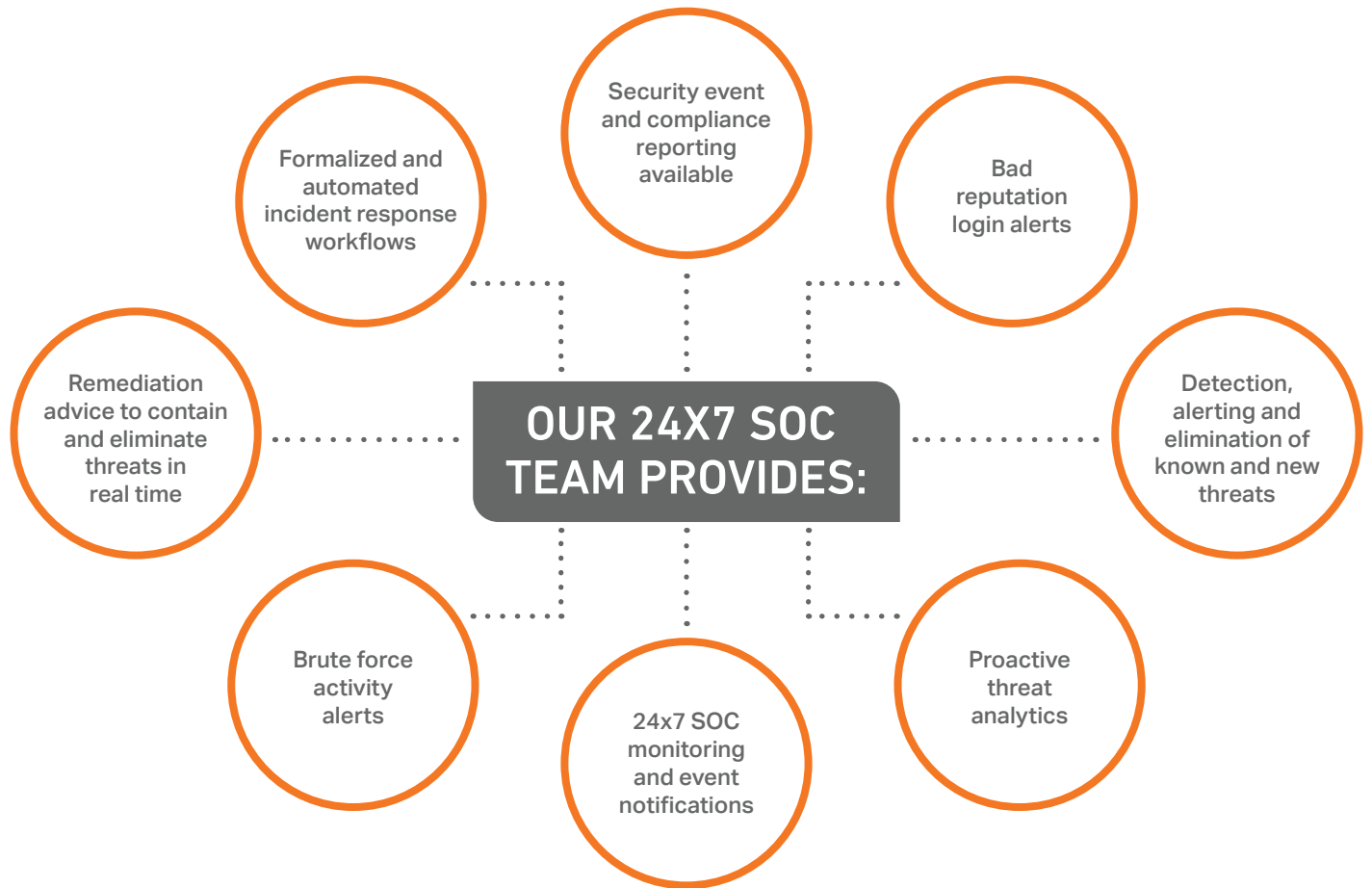
Big data processing

Eliminate blind spots

Preserve data collection

Our SOC team leverages our AI-Driven Open XDR SIEM to provide proactive threat analytics and automatic remediation for your firewall, servers and other devices.

- Logs coming from your firewall and servers
- Network traffic from your switch(es) tap/mirror port
- Data from additional devices

Formalized and automated incident response workflows

Security event and compliance reporting available

Bad reputation login alerts

Remediation advice to contain and eliminate threats in real time

OUR 24X7 SOC TEAM PROVIDES:

Detection, alerting and elimination of known and new threats

Brute force activity alerts

24x7 SOC monitoring and event notifications

Proactive threat analytics

About SonicWall

SonicWall delivers stable, scalable, seamless cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

Datasheet-NDR-SIEM-SOCaas-JK-10136