Security for SMBs

Data Sheet

BL King Consulting

ADVANCED NETWORK DEFENSE

Taking breach prevention to the next level

STOP BREACHES. MONITOR ALL COMPUTER, SERVER, AND NETWORK ACTIVITY 24X7 WITH MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

Bl King Consulting's Advanced Network Defenses Monitor All Of Your Systems Activity With Artificial Intelligence To Stop Attacks Dead In Their Tracks. Activity Fused With Open-Source Threat Intelligence Identifies Attacks From Their Very First Ping.

Key Service Capabilities

AI-Powered Detection

- Combs through billions of activity records every day.
- Identifies anomalous activity that indicates reconnaissance.
- Finds the indicators of compromise (IOC) that humans would otherwise miss.
- Human monitored from a single pane of glass.

Intelligent Prevention

- Prevent malware and ransomware from executing
- Stop advanced threats with malicious behavior, memory threat , and credential hardening protections
- Stop threats targeting cloud workloads and cloud-native applications
- Disrupt advanced threats with behavior-based prevention

Rapid Response

- Rapid response starts with collecting system details and automated host-risk analysis,
- Accelerated remediation with built in remote response actions.
- Detailed activity records enable analysts to quickly identify foot-holds and attack types.

Forensic Analysis

- Billions of activity records enable analysts to confidently identify all systems and files involved in the attack.
- Attribution may prove vital in law enforcement activities, defense department reporting, and corporate espionage litigation.

KEY BENEFITS

- Stop Attacks Before They Start
- Isolate And Contain Ransomware
- Identify Weaknesses
- Shore Up Defenses
- Comply With Governance (CMMC, PCI DSS, Insurance)
- Protect Your Customers Data
- Meet And Maintain Cyber Insurance Requirements
- Correlated Activity Logs with Open Source Threat Intelligence in Real-Time

Security for SMBs

BL King Consulting

MILITARY GRADE CYBERSECURITY FOR YOUR SMB. FORTIFYING YOUR SYSTEMS FROM HACKERS

BL King Consulting's service offerings are built specifically to support CMMC and NIST 800-171 for the remote worker and office worker alike. These security controls can be applied to any SMB but are required for DoD contractors. With similarity to PCS/DSS and ISO 27001, we can ensure compliance with those governance requirements too.

Security Operations Center

- 24x7 AI monitoring
- Staffed 8x5 for AMB budgets
- Fused with open source threat intelligence
- Single most expensive implementation
- Most important for reducing time to notice an attack

Training And Breach Testing/Monitoring

- Training tailored to each individual's level of knowledge
- Extensive catalog
- 3-5 Minutes each prevents training burnout
- Extensive catalog of phishing pages
- Phishing based on real world examples
- Identify and educate employees
- Monitoring the dark web for your employees company email addresses

Unlimited Incident Response

- We respond and continue through all phases of the incident to include a thorough after action analysis
- After action analysis required for reporting or understanding the full effects of an attack could take weeks
- No surprise charges for incident response
- We respond within minutes of initial notification
- We're committed to you through the duration of the incident

Vulnerability And Patch Management

- The #1 best defense is patch management
- All attacks start by exploiting a weakness that usually has a patch available
- Not all patches are applied by patch management systems
- 3rd party patches are not always updated by their auto-update system
- Vulnerability scanning finds missing patches and alerts staff to weaknesses

Cloud Collaboration And Server Monitoring

- Just because it's in the cloud doesn't mean its secure
- Our technology monitors Google, Microsoft, and Amazon for misconfiguration and attacks using the same technology we deploy on your computers
- Adds network monitoring (intrusion detection) to your cloud infrastructure

Continuous Monitoring

- Software and hardware baseline auditing ensures that only approved software is installed, reducing your attack surface
- Governance and policy auditing ensures your policies reflect what is actually happening and corrects deficiencies in processes

ABOUT CMMC

- DoD Security Requirements Policy For Contractors That Process DoD Information
- Compliments DFARS 252.204-7012
- 3rd Party Audit
- In Contracts About Q3FY24
- 2 Levels
  - Level 1
    - Federal Contract Information (FCI)
  - Level 2
    - Controlled Unclassified Information (CUI)
- Uses NIST SP 800-171 And SP 800-171a
- Nist SP 800-171 Revision 3 Is New And Has Significant Changes
- Great Governance For SMBs With No Other Governance Requirements