Brillio iNSOC: Transforming Intelligent Network and Security Operations

brillio

The Growing Need for Intelligent Network & Security Operations

As businesses navigate an increasingly interconnected world, the rise in sophisticated cyber threats underscores the urgency for intelligent, adaptive network and security operations. Modern organizations require solutions that not only address immediate vulnerabilities but also future-proof their digital environments against evolving risks. These demands have reshaped the priorities for network and security management, emphasizing:

- **Real-Time Visibility and Control**
- **Multi-Layered Defense Mechanisms**
- **Centralized Threat Management**
- **Advanced Authentication Systems**
- **Continuous Threat Adaptation**
- **Resilient Infrastructure**

Industry Challenges in Modernizing Network & Security Posture

Traditional security frameworks struggle to provide comprehensive visibility, leading to blind spots that delay threat detection and response. Additionally, conventional defenses often fall short in addressing sophisticated threats across hybrid environments.

Security teams are overwhelmed by excessive alerts from disparate systems, making it difficult to prioritize genuine risks. Insufficient multi-factor authentication protocols further expose networks, especially in remote work. Many organizations also remain stuck in reactive security models. Finally, network outages pose severe financial risks, with unplanned disruptions costing up to $1 million per hour in lost revenue and operational losses.

Recent statistics paint a stark picture of the escalating cybersecurity challenge:

- **88% of organizations** encountered spear-phishing attacks between 2020 and 2021

- Malware attacks **surged by 358%** and ransomware incidents by **435% increase** in 2021 alone.

- Cybercrime now costs organizations **$2.9 million every minute**, with data breaches accounting for **$25 per minute.**

- **Only 37%** of enterprise teams have fully converged NetSecOps teams, with a mere **26% of tools** being shared between NOC and SOC operations.

- **45% of network** device configuration remains manual.

In this volatile digital ecosystem, the message is clear: organizations must embrace intelligent security operations that proactively shield their assets, reputation, and stakeholder relationships.

Comprehensive iNSOC Solution Portfolio

Our comprehensive iNSOC solution modernizes your security operations through intelligent automation and integration, delivering enhanced protection, improved productivity, and sustained operational resilience, ensuring business continuity while optimizing resource utilization.

End-User Security and Access Management: Our unified platform delivers seamless user experiences through role-based access control, balancing security with accessibility, accelerating business processes while maintaining stringent security protocols.

Next-Generation Cloud Network Infrastructure: We integrate cutting-edge SDN with SASE architecture, creating a robust foundation for modern enterprises. Our solution includes automated configuration management and edge computing capabilities, delivering ultra-low latency for mission-critical applications.

AI/ML-Powered Threat Intelligence: Advanced artificial intelligence and machine learning algorithms power our threat detection and response systems, enabling:

- Rapid threat identification and containment
- Real-time security monitoring and analysis

- Automated anomaly detection and response
- Predictive threat modeling and prevention

Strategic Vulnerability Management: Our proactive approach combines regular security testing with custom-developed tools and frameworks, supported by industry experts who ensure your defenses evolve ahead of emerging threats.

Real-Time Thread Detection: By integrating network and security operations, we eliminate silos and enable coordinated incident management, reducing alert fatigue while ensuring priority threats receive immediate attention.

Brillio's Proprietary Approach to Security
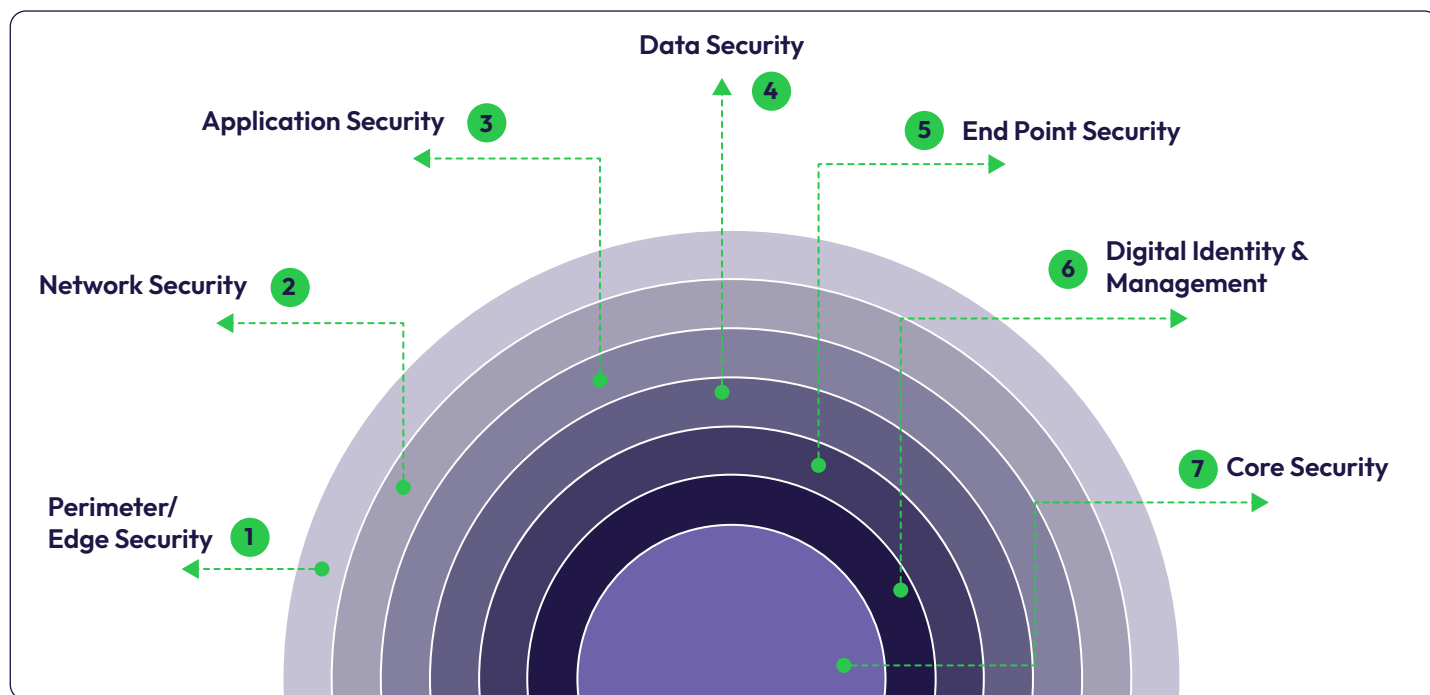
Data Security – At the core of our security framework, BrillioOne.ai works in concert with Microsoft Identification Protection and Thales Data Protection to create an unbreakable shield around your sensitive data, preventing unauthorized access while enabling legitimate business operations.

Application Security – Multi-faceted application security strategy incorporating:

- **Static and Dynamic Testing:** We employ industry-leading tools including BurpSuite, Checkmarx, and Synopsys to conduct comprehensive vulnerability assessments.

- **Runtime Protection:** Leveraging Imperva and Signal Science, we provide real-time application defense against emerging threats and zero-day attacks.

- **Cloud Security:** Through partnerships with Palo Alto and Orca Security, we deliver robust cloud security posture management and workload protection, securing your cloud-native applications.

Network Security – Network defense architecture encompassing:

- **Web Application Defense:** Implementation of enterprise-grade WAF solutions from Cloudflare, Cloud Native, and Akamai to protect against web-based attacks.

- **Wireless Network Protection:** Deployment of Aruba and Cisco WIPS solutions to secure wireless infrastructure against unauthorized access and attacks.

- **Communication Security:** Integration of MimeCast and Proofpoint to protect enterprise communications from advanced threats.

Perimeter and Edge Security– We fortify your network boundaries through:

- **DDoS Mitigation:** Implementing robust protection using Cloud Native, Arbor, and Cloudflare to maintain service availability under attack conditions.

- **Advanced Edge Security:** Deploying comprehensive SSE/Firewall solutions powered by industry leaders including Palo Alto, Juniper, FortiGate, Zscaler, and Netskope.

Endpoint Security Management – Our endpoint protection strategy utilizes best-in-class solutions from Microsoft Windows ATP, CrowdStrike, Trend Micro, McAfee, Sophos, and Symantec to create a robust defense against endpoint-targeted attacks.

Digital Identity Architecture – We implement advanced identity management through:

- **Identity and Access Management (IAM):** Ensure secure user authentication and authorization with Azure AD and OKTA**.**

- **Identity Governance and Administration (IGA):** Streamline access provisioning using SailPoint and Saviynt.

- **Cloud Infrastructure Entitlement Management (CIEM):** Fortify cloud environments with Microsoft Cloudknox and BrillioOne.ai.

Core Security Operations – Our foundational security services include:

- **Vulnerability Assessment and Pen Testing (VAPT):** Identify and address vulnerabilities with tools like Netsparker, Nexpose, Metasploit, Nmap, and OpenSSL.

- **Dark Web Monitoring:** Proactively monitor potential threats and breaches on the dark web to stay ahead of attackers.

Real-World Impact: How Brillio's iNSOC Secures and Transforms Businesses

1.   End-User Security and Access Management
Brillio's iNSOC simplifies and secures user interactions by unifying user registration, login, and self-care experiences while centralizing directory services, authentication, and authorization processes. Advanced multi-factor authentication and role-based access controls limit exposure risks for highly privileged credentials and ensure precise access management.

Business Benefits

- Up to **45% reduction** in the cost of managing Identity and Access Management (IAM).

- Up to **30% faster** access to business applications.

- Up to **50% improvement** in user productivity.

2. Cloud-Delivered Network & Security Platform
Brillio's iNSOC enables secure, scalable operations by consolidating multiple security functions into a single, cloud-native service. With context-aware AIOps for dynamic configuration, Zero Trust architecture replaces complex VPNs, while centralized policy management ensures seamless protection against malware and network attacks. Controlled data migration supports a smooth transition to cloud infrastructure.

Business Benefits

- Identity-based **Zero Trust** network access and seamless convergence of network and security.

- Protection against attacks on network infrastructure.

- Prevention of malware-based attacks and data exfiltration of corporate information.

3. Improved Security Incident Response Powered by AI/ML Models

With Brillio's iNSOC, organizations achieve faster and more effective threat detection through centralized governance of security systems. AI/ML models analyze and correlate data across emails, endpoints, and cloud workloads to prioritize and remediate threats, strengthening response capabilities and securing digital assets inside and beyond the traditional network perimeter.

Business Benefits

- Enhanced protection, detection, and response capabilities.

- Up to **30% improvement** in security team productivity.

- Lower total cost of ownership for effective threat detection and response.

4. Identifying and Addressing Security Vulnerabilities

Brillio's iNSOC proactively identifies key vulnerabilities and configuration issues, offering actionable guidance for remediation. Comprehensive security assessments, detailed reports, and adversarial simulations improve the organization's ability to detect and respond to threats, providing a holistic view of weaknesses in networks and applications.

Business Benefits

- Comprehensive view of potential threats in networks and applications.

- Identification of programming errors that could lead to cyberattacks.

- Holistic vulnerability reports for the overall infrastructure.

5. Real-Time Threat Detection

By collecting and analyzing security logs from systems, devices, and applications, Brillio's iNSOC ensures real-time detection of anomalies. Enhanced by AI/ML capabilities, this automated monitoring approach notifies security teams promptly to reduce Priority 1 incidents and improve response times.

Business Benefits

- Automated monitoring of users and applications.

- Up to 25% faster response to security-related alerts.

- Up to 38% reduction in Priority 1 (P1) security incidents.

What You Gain with Brillio's INSOC Solutions

Brillio's iNSOC represents a paradigm shift in managing network and security operations, delivering a unified defense system that strengthens security posture while driving operational excellence. Our integrated approach transforms organizations through:

- **Faster Response Time:** Reduce the time taken to detect, investigate, and respond to threats with a combined network and security approach.

- **Increased Productivity:** Automate onboarding and orchestration of network devices to eliminate manual inefficiencies.

- **Enhanced Efficiency:** Optimize operational and cost efficiencies through integrated incident management and identity access controls.

- **Strengthened Security Posture:** Implement comprehensive tools and processes to proactively identify, prioritize, and mitigate risks.

brillio

ABOUT BRILLIO

At Brillio, our customers are at the heart of everything we do. We were founded on the philosophy that to be great at something, you need to be unreasonably focused. That's why we are relentless about delivering the technology-enabled solutions our customers need to thrive in today's digital economy. Simply put, we help our customers accelerate what matters to their business by leveraging our expertise in agile engineering to bring human-centric products to market at warp speed. Born in the digital age, we embrace the four superpowers of technology, enabling our customers to not only improve their current performance but to rethink their business in entirely new ways. Headquartered in Silicon Valley, Brillio has exceptional employees worldwide and is trusted by hundreds of Fortune 2000 organizations across the globe.

https://www.brillio.com/
Contact Us: info@brillio.com