BNETAL™
bnetal.com

Advisory Security Consulting Services Profile

Security is mission critical for your business.

Let us apply our experience from leading financial, banking and tax advisory consulting security engagements to protect your data from a growing set of threats.

- Security Architecture Gap Assessments
- Identification and selection of best of breed solutions
- Definition of Adoption Roadmaps
- Zero Trust
- Network micro-segmentation, SD-WAN
- Tokenization
- M&A Security Roadmap, Solutioning
- Enterprise and Cloud Security Architecture
- Regulatory Compliance
- Security Baseline Definition
- Security Gap Assessments
- Identity & Access Governance
- Identity Federation
- Multi-factor Authentication
- Single Sign-on
- API Security
- Data Loss Prevention
- Endpoint Protection
- Web Application Firewall
- Log Ingestion and Aggregation
- Data Classification
- Security Posture Management
- API Security
- Data Isolation
- Unstructured data classification
- Encryption Key Management

BNETAL™
bnetal.com

Advisory Security Consulting Services Profile

Security Baseline / Policy Definition

A security baseline is a set of minimum-security standards and configurations that an organization must adhere to. BNETAL has been engaged to develop security baselines for major cloud and on-prem projects (e.g., EY Azure based Global Tax Platform, Santander M&A, NC DHHS AWS). Ensuring that baselines help lower organizational risks, meet regulatory requirements and organizational policies while enabling business and facilitating time to market are important considerations in developing baselines.

Security Posture

Security posture refers to the overall state of an organization's security practices and defenses. It encompasses the effectiveness of security controls, the presence of vulnerabilities, and the organization's ability to detect and respond to threats. BNETAL security consultants have been engaged to define, refine or assess security postures of various client organizations in financial and healthcare domains. Security posture helps formulate strong risk management and governance programs and enables development and refinement of policies and adoption of standards to enforce the posture.

Security Architecture Gap Assessments

A security architecture gap assessment is a systematic process to identify discrepancies between an organization's current security posture and its desired security objectives.. BNETAL has performed several security gap assessments at infrastructure, services and application levels, and helped its clients in prioritizing the gaps identified using a risk- based approach. BNETAL helped senior leadership in client organizations with making risk management decisions based on careful and thoughtful considerations of objectives and risks.

Security Solution Selection and Roadmap Definition

Selecting the right security solutions and defining a clear roadmap is crucial for safeguarding an organization's assets and mitigating risks. BNETAL has been instrumental in helping its clients identify solution options for gap remediation, including vendor product selection to meet requirements by doing pros and cons analysis among a range of options. Once solutions are selected, BNETAL works with client stakeholders to define roadmaps for solution implementation, taking into consideration other competing enterprise priorities and roadmaps. Our experience, combined with thoughtful and professional approach to reason about complex problems and build consensus on tactical and strategic solution approaches has been greatly appreciated by C level leaders in various client organizations.

BNETAL™
bnetal.com

Advisory Security Consulting Services Profile

Zero Trust

Zero Trust is a security model that assumes that any device, user, or application accessing the network is potentially a threat. It shifts the traditional perimeter-based security approach to a trust-nothing model, requiring strict verification and authorization for every access request. At a major bank, BNETAL was engaged in a Zero Trust initiative that helped reduce the overall risk while improving security posture. BNETAL is working with a major European company on their Zero Trust roadmap and solutions. Among other things, use of multi-factor authentication, cloud native identity federation and other techniques were used by BNETAL to help our clients move towards Zero Trust.

Network Micro-Segmentation

Network micro-segmentation is a security strategy that divides a network into smaller, isolated segments to limit the potential impact of a security breach. By breaking down the network into smaller, more manageable units, organizations can reduce the lateral movement of attackers and prevent them from spreading to critical systems. BNETAL was engaged by a major European bank to help define network zones with micro-segmentation when integrating the network of a broker dealer. BNETAL is currently working with a major European company to help use SD-WAN as a network overlay technology to enforce network micro-segmentation.

Blockchain

Blockchain is a distributed ledger technology (DLT) that records data in a way that makes it difficult or impossible to modify, hack, or cheat the system. It is a growing field with potential applications in various industries. Using its strong foundation of R&D in cryptographic protocols and accountability in electronic commerce, BNETAL consultants have been assisting our clients formulate their strategy for adoption and leveraging blockchain as a business enabler.

Tokenization

Bank tokenization is a security measure that replaces sensitive card data, such as credit or debit card numbers, with unique, non-sensitive tokens. These tokens are then used for subsequent transactions, protecting the original card data from unauthorized access or misuse. Applying its extensive background in data anonymization, BNETAL helps its clients to define a tokenization strategy and roadmap, to help improve data security and privacy while supporting business functionality.

BNETAL™
bnetal.com

Advisory Security Consulting Services Profile

Observability and Security

Observability and security are two interconnected concepts that are crucial for organizations to maintain a strong security posture. Observability provides the visibility needed to understand the behavior of systems and applications, while security measures protect those systems from threats. BNETAL consultants experience in security observability is through the system performance tools like DynaTrace and security tools such as Cloud Security Posture Management (CSPM) tools (e.g., SysDig), vulnerability scanning tools (e.g., Nessus).

Cloud Security

Cloud security is a critical aspect of modern IT infrastructure, as more and more organizations are adopting cloud-based services. It involves safeguarding data, applications, and infrastructure from unauthorized access, threats, and vulnerabilities in the cloud environment. BNETAL's cloud security experience ranges from all major cloud services providers (AWS, Azure, GCP), cloud models (SaaS, PaaS, IaaS), public and private clouds and hybrid on-prem and cloud hosting models. Our projects for EY, Santander, NC DHHS and other clients have been cloud based, and we played the role of thought leaders and security architects.

Cloud Security Posture Management

Cloud Security Posture Management (CSPM) is a comprehensive approach to assessing, monitoring, and improving the security posture of cloud environments. It helps organizations identify and address vulnerabilities, ensure compliance with regulations, and maintain a high level of security in their cloud deployments. BNETAL has been engaged on projects wherein CSPM tools like Dome9 and SysDig have been used to assess the security baseline compliance of client cloud environments. Gaps found from these CSPM assessments were remediated with guidance from BNETAL, and validated via new scans.

Endpoint Protection

Endpoint protection is a critical component of cybersecurity that involves safeguarding individual devices, such as computers, laptops, smartphones, and tablets, from various threats. These threats can include malware, viruses, spyware, ransomware, and unauthorized access. At a major European bank, BNETAL provided solution architecture for CrowdStrike, McAfee and other endpoint protection technologies.

BNETAL™
bnetal.com

Advisory Security Consulting Services Profile

Business Transformation Security (e.g., M&A, Infrastructure Migration)

Business transformation can involve significant changes to an organization's processes, technology, or structure. These transformations often introduce new risks and vulnerabilities that must be carefully addressed to ensure the security of sensitive data and systems. BNETAL's security consultants have advised CISOs of banks, big4 firms and state departments of health on various business transformation initiatives and their impact on security. This includes mergers and acquisitions, and migration from on-premise infrastructure to cloud. Our seasoned, thoughtful and professional approach to reason about difficult problems and build consensus on tactical and strategic solution approaches has been greatly appreciated by C level leaders in various client organizations.

Data Loss Prevention

Data Loss Prevention (DLP) is a security strategy designed to prevent sensitive data from being exfiltrated from an organization's network. DLP solutions monitor data flows, identify sensitive information, and implement measures to prevent unauthorized access, transmission, or loss. At a major European bank, BNETAL engineers lead the implementation of various DLP technologies for endpoint and email DLP.

Identity and Access Governance, Management, Federation

Identity and Access Governance (IAG) is a comprehensive approach to managing user identities, access rights, and privileges within an organization. It ensures that only authorized individuals have access to the resources and data they need to perform their job functions. Identity federation is a mechanism that allows users to access multiple applications and services using a single set of credentials. It simplifies the login process for users and reduces the risk of credential theft. BNETAL has in-depth expertise and experience in all aspects of Identity lifecyels including Access Governance, and identity federation standards including WS-Fed, OAuth2, OIDC, SAML2 and technologies including Azure AD, Ping Federate, Netegrity and BNETAL ManageSecure.

Security Regulatory Compliance

Security compliance is the process of ensuring that an organization adheres to specific security standards, laws, and regulations. It is essential for protecting sensitive data, mitigating risks, and maintaining a positive reputation. BNETAL has done several security assessments within healthcare sector for regulatory requirements such as HIPAA Security & Privacy, NIST 800-63. It has supported platform level SOC2 Type II audits, and within banking and finance, it has gone through SOX, GLBA and GDPR compliance assessments.