Solution Brief

Intel Security and TCS: Together Securing Workloads of the Modern Data Center

Data center security today is extremely different from what it was an era ago—primarily because the data center has undergone a huge transformation. Most organizations are consolidating their data centers with virtualization into private clouds or migrating workloads to public clouds as a way of reducing the overall cost of data center implementation and maintenance. Mobility and Big Data are the other disruptors that are changing the way data centers are being developed and managed.

TATA
TATA CONSULTANCY SERVICES

What Are the Security Challenges Posed by This Transformation?

With these transformations, securing the modern data center has to be fundamentally reinvented to address the following challenges:

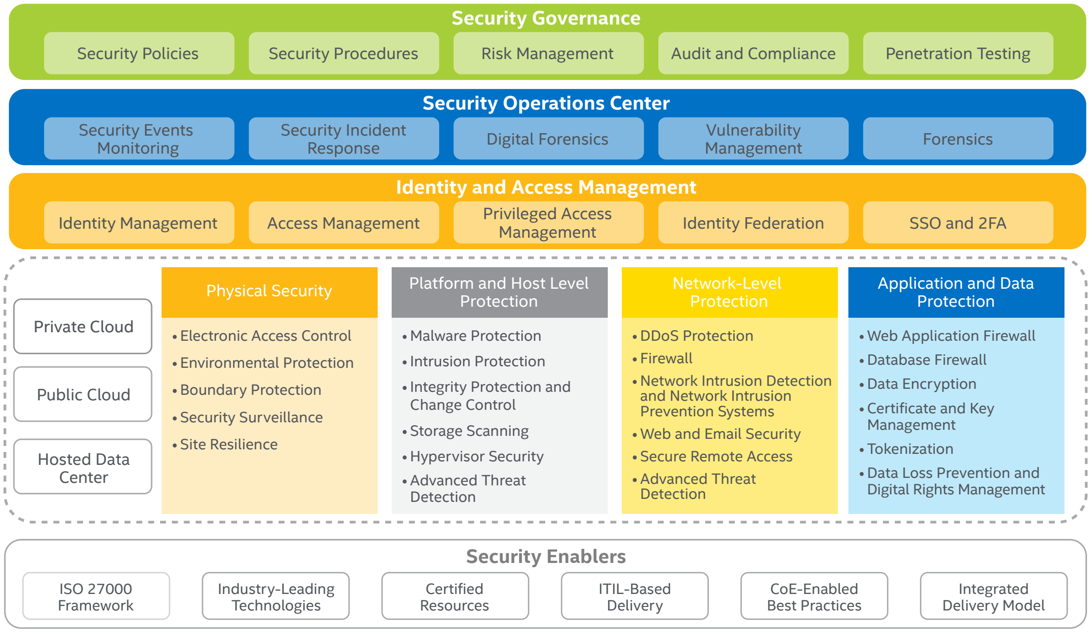
- **Governance and compliance:** Due to adoption of the cloud model and limited control on data center assets, security teams face challenges to ensure effective enforcement of security controls.
- **Consolidation and convergence technologies:** With increasing virtualization, security is losing visibility on inter- and intra-virtual machine (VM) traffic, and, as a consequence, IT is finding it difficult to enforce controls to ensure security.
- **Increased threat exposure:** Modern data centers are called upon to provide seamless access to hosted application using mobile devices. This creates additional channels for hackers to get into the data center network.
- **Protection of data dispersed across multiple locations:** Data associated with workloads is available at multiple places and it is difficult to protect data wherever it resides due to lack of complete control.
- **Managing identity and access:** With the increasing consumerization of IT services, managing and maintaining right level of access in a data center environment is also one of the time-consuming tasks of security teams.
- **Disparate security solution:** There are multiple security technology solutions from multiple vendors that do not talk to each other and fail to deliver the best protection and operational efficiency.

intel Security

The TCS Data Center Security Framework for the Modern Data Center

Tata Consultancy Services (TCS) offers a comprehensive, integrated data center security framework that addresses security controls at each layer—physical, host and platform, network, and application. The framework helps organizations strike a balance between security controls and operating expenses to ensure efficient risk management. The key TCS enablers for delivering data center security include:

1. **An integrated security ecosystem:** TCS deploys industry-leading security technologies that exchange intelligence across endpoints and networks in near real time to deliver automated, adaptive, and enhanced protection.
2. **Technology alliances and center of excellence ecosystem (CoE):** TCS has solution and product-specific CoEs that enable access to best practices, technical reference materials from vendors, and ad-hoc training for additional staff for faster deployment of projects.
3. **Quality management practices:** By leveraging the right-shore delivery and resource model and risk-based security approach, TCS provides convenience and compliance while reducing costs. All our data centers are certified for ISO 9000, CMMi Level 5, PCMM Level 5, ISO 20000, and ISO 27001.
4. **A comprehensive security experience:** TCS has comprehensive security engagement experience for security operations, along with depth and breadth of expertise in multilayer security products and specialized teams who focus on penetration testing, incident response, and digital forensics
5. **Risk-averse execution:** Customized execution approach comprising rapid, incremental, and measurable steps. The primary objective is to manage risk without any disruption to current service levels and the customer experience.



Security Governance

Security Policies | Security Procedures | Risk Management | Audit and Compliance | Penetration Testing

Security Operations Center

Security Events Monitoring | Security Incident Response | Digital Forensics | Vulnerability Management | Forensics

Identity and Access Management

Identity Management | Access Management | Privileged Access Management | Identity Federation | SSO and 2FA

Private Cloud

Public Cloud

Hosted Data Center

Physical Security
- Electronic Access Control
- Environmental Protection
- Boundary Protection
- Security Surveillance
- Site Resilience

Platform and Host Level Protection
- Malware Protection
- Intrusion Protection
- Integrity Protection and Change Control
- Storage Scanning
- Hypervisor Security
- Advanced Threat Detection

Network-Level Protection
- DDoS Protection
- Firewall
- Network Intrusion Detection and Network Intrusion Prevention Systems
- Web and Email Security
- Secure Remote Access
- Advanced Threat Detection

Application and Data Protection
- Web Application Firewall
- Database Firewall
- Data Encryption
- Certificate and Key Management
- Tokenization
- Data Loss Prevention and Digital Rights Management

Security Enablers

ISO 27000 Framework | Industry-Leading Technologies | Certified Resources | ITIL-Based Delivery | CoE-Enabled Best Practices | Integrated Delivery Model

Figure 1. The TCS Data Center Security Framework: a logical view.

Intel Security Powers the TCS Data Center Security Framework

Intel Security provides a portfolio of capabilities with an integrated approach to security that begins with security fundamentals and moves up to more advanced security implementations for total security protection. Taking this approach allows IT security administrators to clearly define what their security strategy should be for next-generation data centers and how they can ensure success in mitigating risk.

Platform and Host-Level Protection

Through integration with Intel Security's technologies, the TCS Data Center Security Framework delivers operating system, middleware, and application protection for workloads, regardless of their location in legacy data centers, private clouds, or public clouds. With support for software-defined security, the solution can dynamically protect workloads based on industry best practices and compliant with regulatory requirements like PCI-DSS. Key offerings include:

- TCS Managed Platform and Host Protection (Basic) with McAfee® Server Security Essentials (malware Protection and intrusion protection).
- TCS Managed Platform and Host Protection (Advanced) with McAfee Server Security Advanced (malware, intrusion, and integrity protection) and McAfee VirusScan® Enterprise for Storage (storage scanning).
- TCS Managed Advanced Threat Detection for Servers (add-on service) with McAfee Threat Intelligence Exchange and McAfee Advanced Threat Defense.

Joint solution benefits

- Single-console management for multiple products through McAfee® ePolicy Orchestrator® (McAfee ePO™) software across physical, virtual, and cloud environments
- Tiered service levels for protection controls based on enterprise risk profile.
- Best-in-class technologies combined with industry leadership and proven performance.
- Protection that goes beyond signatures, offering the ability to protect against targeted and zero-day attacks.

Platform and Host-Level Protection

- Malware protection.
- Intrusion protection.
- Integrity protection and change control.
- Storage scanning.
- Hypervisor security.
- Advanced threat detection.

Network-Level Protection

Intel Security's technologies and the TCS Data Center Security Framework deliver threat prevention for physical and virtual networks and also provides a secure web experience for corporate users. With support for software-defined security, the solution dynamically adapts to motion of workloads across data centers for adaptive network breach defense. Key offerings include:

- Managed network intrusion prevention with McAfee Network Security Platform (network intrusion detection, network intrusion prevention, and DDoS protection).
- Managed web security with McAfee Web Protection—on-premise, SaaS, or hybrid deployments.
- Add-on service: Managed Breach Defense with McAfee Advanced Threat Defense.

Joint solution benefits

- Fine-grained network and content security with content, identity, and application awareness.
- Advanced breach detection and defense using signature-based and advanced signature-less techniques.
- Flexibility of deployment as purpose-built high-performance appliances or as virtual appliances in software-defined data centers.
- Best-in-class technologies with industry leadership and proven performance of network and content-based threat prevention.

Network-Level Protection

- DDoS protection.
- Firewall.
- Network intrusion detection/network intrusion prevention.
- Web security.
- Secure remote access.
- Advanced threat detection.

Data Protection

In collaboration with Intel Security's technologies, the TCS Data Center Security Framework delivers comprehensive data protection and data loss prevention—from data stores residing on file shares or on databases. With support for mobility, the solution not only allows a secure user experience, but also identifies and prevents insider threats. Key offerings include:

- TCS Managed Encryption Services with McAfee Complete Data Protection (drive encryption and file and removable media encryption).
- TCS Managed Data Loss Prevention with McAfee Data Loss Prevention Endpoint and McAfee Network Data Loss Prevention.
- TCS Managed Database Protection with McAfee Data Center Security Suite for Databases (database activity monitoring, virtual patching, and vulnerability management for databases).

Joint solution benefits

- Common management console (McAfee ePO software) to manage platforms and data protection services.
- User-friendly security controls with fine-grained policies to balance user experience with security.
- Holistic prevention of data theft via stolen devices or network breaches, with forensic evidence of behavior.
- Easily extended to virtual environments (such as VDI) and cloud environments through risk-based policies.

Data Protection

- Database firewall.
- Data encryption.
- Data loss prevention and data.

Security Operations Center

Intel Security technologies and the TCS Data Center Security Framework deliver comprehensive threat visibility and incident management, including post-incident analysis and forensics. Supporting multiple sources of threat intelligence, custom correlation logic, and analytical workflows for incident investigation, the solution delivers and acts on rich security intelligence to contain and mitigate threats. Key offerings include:

- TCS Managed SIEM Foundation with McAfee Enterprise Security Manager, McAfee Enterprise Log Manager, and McAfee Event Receiver.
- TCS Managed SIEM—Situational Awareness with McAfee Enterprise Security Manager, McAfee Enterprise Log Manager, McAfee Enterprise Receiver, McAfee Advanced Correlation Engine and McAfee Global Threat Intelligence for McAfee Enterprise Security Manager.
- TCS Add-On Services: TCS Managed SIEM Situational Awareness for Applications and Databases with McAfee Application Data Monitor and McAfee Database Event Monitor

Joint solution benefits

- Single console visibility for situational awareness, incident detection, and analytics across the enterprise.
- Flexible, scalable, and resilient architecture to support security Big Data and detection of targeted attacks.
- Ability to automate orchestration of incident response actions on the network and on endpoints.
- Advanced content packs tailored for customer requirements based on functional use cases.

Security Operations Center

- Security events monitoring.
- Security incident response.
- Digital forensics.
- Vulnerability management.
- Forensics.

Partnering for Success: Intel Security and TCS

Intel Security and TCS have partnered on numerous large engagements to deliver strategic security services—from managed endpoint security to managed SIEM services. The success of this partnership is built on the TCS Global Delivery Model, which effectively delivers managed security services and the Intel Security solution portfolio and enables TCS with the right technologies to protect customer environments. Together, Intel Security and TCS protect more than 1.3 million endpoints and 100 global organizations across a wide variety of industry verticals, including banking and finance, energy and utilities, transportation, manufacturing, retail, and healthcare.

About Tata Consultancy Services

Tata Consultancy Services (TCS) is an IT services consulting and business solutions organization that delivers real results to global businesses, ensuring a level of certainty no other firm can match. TCS ESRM (Enterprise Security and Risk Management) offers end-to-end security services covering consulting, professional services, and operations support. Our integrated, analytics-driven, metrics-based Managed Security Services (MSS) offerings ensure optimal protection, effective incident response, and threat management. Leveraging the security operation center (SOC), TCS and Intel Security collaborate on delivering integrated, automated, and effective security services to keep your IT security a step ahead of the hackers.

http://www.tcs.com/enterprise-security-risk-management/Pages/default.aspx

TCS Security Expertise

- More than 200 subject matter experts.
- Protecting more than 1.3 million endpoints.
- Analyzing more than 2.05 billion security event records every day.
- Securing more than 100 customers across the globe.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com