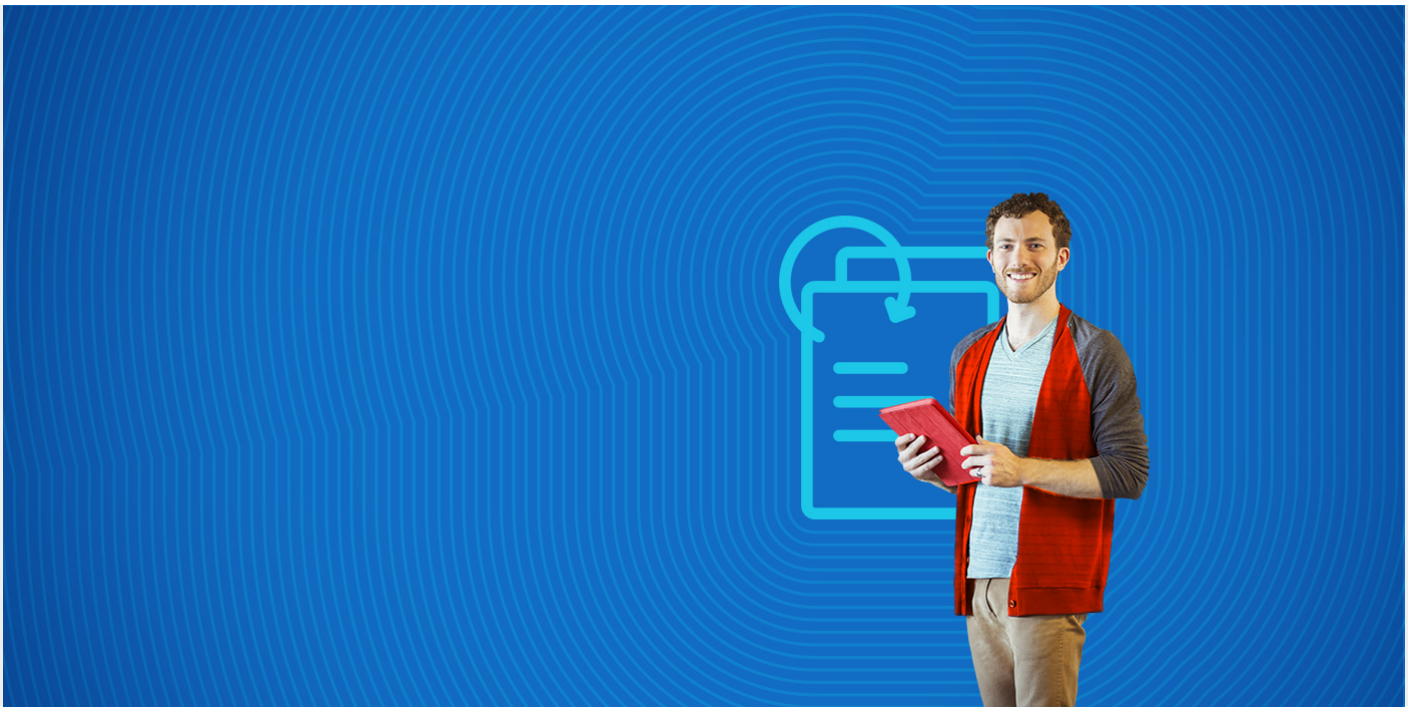
INTRODUCTION TO ENTERPRISE SECURITY



The attack surface of any enterprise has expanded significantly in recent years. Traditionally, organizations would be responsible for securing data stored in on-premise servers and leverage state-of-the-art security solutions to protect against cyber-attacks. These threats were usually motivated by financial or political gains. Today, businesses connect technologies to reach a wider user base, collaborate with vendors, and allow for work across a distributed workforce across geographically disparate locations—your risk is higher than ever before.

The growing attack surface requires defense systems that go beyond traditional cybersecurity measures. Let's take a look at enterprise security.

(This article is part of our Security & Compliance Guide. Use the right-hand menu to navigate.)

What is Enterprise Security?

Enterprise Security includes the strategies, techniques, and process of securing information and IT assets against unauthorized access and risks that may infringe the confidentiality, integrity or availability of these systems. Building on the traditional cybersecurity premise of protecting digital assets at the local front, enterprise security extends to the security of data in transit across the connected network, servers, and end-users.

It encompasses the technology, people, and processes involved in maintaining a secure environment for digital assets. Because it encompasses the enterprise, this security has additional focus on the legal and cultural requirements of securing data assets that belong to an organization's user base.

Enhancing cybersecurity measures for the enterprise

The following trends are forcing organizations to enhance their cybersecurity measures across all levels of the enterprise:

The cloud

The proliferation of cloud computing has enabled organizations of all sizes to take advantage of high-end and scalable hardware resources at an OpEx basis. As a result, they have been able to expand their business across global markets—but that comes with a significant caveat: a vast volume of data is not accessible to companies, yet they are responsible for securing their data assets.

The trouble with cloud-stored data is significant. The data is not locally hosted. Enterprises do not control the cloud computing resources that store it. With limited visibility and control into cloud hardware, you must rely on cloud vendors for your first line of defense.

The IoT

The influx of connected devices, the Internet of Things, allows businesses to extend their service offerings and achieve operational excellence. IoT has enabled organizations to automate manual processes, reduce human error, and pursue new business models.

The growing ecosystem of IoT networks also brings key challenges:

1. The number of potentially vulnerable devices connecting to the corporate network has increased dramatically.
2. Attackers now have more pathways to exploit as most IoT devices can offer limited security defense at the physical layer of network endpoints.

The drive for data

More data means more insights. Organizations rely on insightful information to deliver the right services to the right customer. Computing resources and data intelligence solutions are widely available and affordable. End-users are willing to share some personal information in exchange for a useful service. This brings tremendous opportunities for enterprises to produce data-driven products and business strategies that guarantee high returns on investments.

At the same time, these companies are responsible for securing user information that must be leveraged *only* for the allowed purposes and within ethical bounds of the modern digital world.

Privacy awareness and regulations

Governments around the world have recognized the need for stringent privacy regulations in response to growing cyber-security risks to end-users. In 2013, all 3 billion Yahoo user accounts were hacked, eventually resulting in a data breach settlement of $117.5 million. More importantly, the company has since lost billions of dollars in market cap as internet users have largely adopted alternatives. The lost brand reputation has been irrecoverable and was caused due to a large-scale data leak that took place long before it was discovered and made public.

More recently, governments have enforced compliance measures that force businesses to reshape and enhance their enterprise security capabilities, along with heavy fines for compliance failure. GDPR in the EU is a prime example.

Best practices for enterprise security

Enterprise security therefore involves security measures across all aspects of the organization. It ranges from backend cloud networks to IoT endpoints at the network edge. It is driven by the proliferation of data-intensive business operations and services, and heavily mandated by stringent global regulations. Internet users are increasingly aware and distant from organizations failing to guarantee security of their personal information.

The threats come from both within the enterprise, such as human error or disgruntled employees, as well as external cyber-attackers. The following best practices can help your organizations improve security capabilities across all these fronts:

- **Protect the data at rest and in transit.** Identify data assets that must be encrypted and develop a security strategy around it. Encryption should scale across your network and secure data workloads in dynamic and distributed cloud environments. Monitor the performance of your encryption implementations.
- **Establish strong Identity and Access Management controls.** Use the principle of least privilege that allows users only the limited necessary access to perform their job. Limiting user access reduces the risk of data leaks and network intrusions via human error or malicious intent.
- **Enact a strong disaster recovery and risk mitigation plan.** A well-defined plan should include responsibilities and workflows for orderly and successful disaster recovery protocols. Update this plan regularly to combat growing cyber threats and changing workforce landscapes.
- **Educate your employees on cybersecurity measures.** The workforce can behave as a strong first line of defense against cyber threats that target the human element. On the other hand,

employees lacking security awareness can serve as weak links in the security chain that's otherwise equipped with advanced security solutions.
- **Manage endpoint security with technologies that monitor network performance continuously for anomalous data traffic.** Ensure that IoT devices are properly configured and operate on up to date firmware.
- **Involve senior management in developing the enterprise security strategy.** Cyber threats should not be treated as or relegated to an "IT only"—it is a business problem that must become a business activity. Security expertise should span the executive level where the necessary risk management decisions must take place. The board and executive management should understand the legal, financial, cultural as well as technology-related implications of their enterprise security decisions.

Additional resources

For more details on securing the modern enterprise, browse our BMC Security & Compliance Blog or check out these articles:

- IT Security & Compliance Introduction
- IT Security Vulnerability vs Threat vs Risk: What Are the Differences?
- Big Data Security Issues in the Enterprise
- Data Breaches: 5 Examples of Data Breaches from 2018
- Disaster Recovery for the Cloud
- IT Disaster Recovery Planning Explained
- Digital Forensics and Incident Response (DFIR): An Introduction