Modern Computing Trends

The nature of enterprise computing has changed dramatically over the past decade. Core business applications are now commonly installed alongside *Web 2.0* apps on a variety of *endpoints*, and networks that were originally designed to share files and printers are now used to collect massive volumes of data, exchange real-time information, transact online business, and enable global collaboration.

Many Web 2.0 apps are available as *software-as-a-service* (SaaS), web-based, or mobile apps that can be easily installed by end users or that can be run without installing any local programs or services on the endpoint. The use of Web 2.0 apps in the enterprise is sometimes referred to as *Enterprise 2.0*, although not all Web 2.0 apps are considered to be Enterprise 2.0 applications.

Key Terms

Web 2.0 is a term popularized by Tim O'Reilly and Dale Dougherty that unofficially refers to a new era of the World Wide Web, which is characterized by dynamic or user-generated content, interaction, and collaboration, as well as the growth of social media.

An *endpoint* is a computing device such as a desktop or laptop computer, handheld scanner, *internet of things* (IoT) device or sensor (such as an autonomous vehicle, smart appliance, smart meter, smart TV, or wearable device), point-of-sale (POS) terminal, printer, satellite radio, security or videoconferencing camera, self-service kiosk, smartphone, tablet, or *Voice over Internet Protocol* (VoIP) phone. Although endpoints can include servers and network equipment, the term is generally used to describe end-user devices.

The *internet of things* (IoT) is the network of physical smart objects that are embedded with electronics, software, sensors, and network connectivity to collect and share data.

Voice over IP (VoIP), or *IP telephony*, is technology that provides voice communication over an Internet Protocol (IP)-based network.

Software as a service (SaaS) is a category of cloud computing services in which the customer is provided access to a hosted application that is maintained by the service provider.

Enterprise 2.0 is a term introduced by Andrew McAfee and defined as "the use of emergent social software platforms within companies, or between companies and their partners or customers."

Typical core business applications include:

Accounting software is used to process and record accounting data and transactions such as accounts payable, accounts receivable, payroll, trial balances, and general ledger (GL) entries. Examples of accounting software include Intacct, Microsoft Dynamics AX and GP, NetSuite, QuickBooks, and Sage.

Business intelligence (BI) and business analytics software consists of tools and techniques used to surface large amounts of raw unstructured data from a variety of sources (such as data warehouses and data marts). BI and business analytics software performs a variety of functions, including business performance management, data mining, event processing, and predictive analytics. Examples of BI and analytics software include IBM Cognos, MicroStrategy, Oracle Hyperion, and SAP.

Content management systems (CMS) and enterprise content management (ECM) systems are used to store and organize files from a central management interface, with features such as indexing, publishing, search, workflow management, and versioning. Examples of CMS and ECM software include EMC Documentum, HP Autonomy, Microsoft SharePoint, and OpenText.

Customer relationship management (CRM) software is used to manage an organization's customer (or client) information, including lead validation, past sales, communication and interaction logs, and service history. Examples of CRM suites include Microsoft Dynamics CRM, Salesforce.com, SugarCRM, and ZOHO.

Database management systems (DBMS) are used to administer databases, including the schemas, tables, queries, reports, views, and other objects that comprise a database. Examples of DBMS software include Microsoft SQL Server, MySQL, NoSQL, and Oracle Database.

Enterprise resource planning (ERP) systems provide an integrated view of core business processes such as product and cost planning, manufacturing or service delivery, inventory management, and shipping and payment. Examples of ERP software include NetSuite, Oracle's JD Edwards EnterpriseOne and PeopleSoft, and SAP.

Enterprise asset management (EAM) software is used to manage an organization's physical assets throughout their entire lifecycle, including acquisition, upgrade, maintenance, repair, replacement, decommissioning, and disposal. EAM is commonly implemented as an integrated module of ERP systems. Examples of EAM software include IBM Maximo, Infor EAM, and SAP.

Supply chain management (SCM) software is used to manage supply chain transactions, supplier relationships, and various business processes, such as purchase order processing, inventory management, and warehouse management. SCM software is commonly integrated with ERP systems. Examples of SCM software include Fishbowl Inventory, Freightview, Infor Supply Chain Management, and Sage X3.

Web content management (WCM) software is used to manage website content, including administration, authoring, collaboration, and publishing. Examples of web content management software include Drupal, IBM FileNet, Joomla, and WordPress.

Common Web 2.0 apps and services (many of which are also SaaS apps) include:

File sync and sharing services are used to manage, distribute, and provide access to online content, such as documents, images, music, software, and video. Examples include Apple iCloud, Box, Dropbox, Google Drive, Microsoft OneDrive, Spotify, and YouTube.

Instant messaging (IM) is used to exchange short messages in real time. Examples include Facebook Messenger, Skype, Snapchat, and WhatsApp.

Microblogging web services allow a subscriber to broadcast short messages to other subscribers. Examples include Tumblr and Twitter.

Office productivity suites consist of cloud-based word processing, spreadsheet, and presentation software. Examples include Google Apps and Microsoft Office 365.

Remote access software is used for remote sharing and control of an endpoint, typically for collaboration or troubleshooting. Examples include LogMeIn and TeamViewer.

Remote team meeting software is used for audio conferencing, video conferencing, and screen sharing. Examples include Adobe Connect, Microsoft Teams, and Zoom.

Social curation shares collaborative content about particular topics. Social bookmarking is a type of social curation. Examples include Cogenz, Instagram, Pinterest, and Reddit.

Social networks are used to share content with business or personal contacts. Examples include Facebook, Google+, and LinkedIn.

Web-based email is an internet email service that is typically accessed via a web browser. Examples include Gmail, Outlook.com, and Yahoo! Mail.

Wikis enable users to contribute, collaborate, and edit site content. Examples include Socialtext and Wikipedia.

According to research from McKinsey & Company and the Association for Information and Image Management (AIIM), many organizations are recognizing significant benefits from the use of Enterprise 2.0 applications and technologies, including better collaboration, increased knowledge sharing, and reduced expenses (for example, for travel, operations, and communications).[1] Thus, enterprise infrastructures (systems, applications, and networks) are rapidly converging with personal and Web 2.0 technologies and apps, making definition of where the internet begins and the enterprise infrastructure ends practically impossible. This convergence is being driven by several important trends, including:

[1] "Application Usage & Risk Report: Fall 2009." Palo Alto Networks. November 2009. https://researchcenter.paloaltonetworks.com/2009/11/application-usage-risk-report-fall-2009/.

Cloud computing. Cloud computing is now more ubiquitous than ever. According to the *RightScale 2019 State of the Cloud Report* from Flexera, *public* and *private cloud* adoption is now at 94 percent for enterprises (1,000+ employees) and small-medium businesses (fewer than 1,000 employees), and those companies run a majority of their workloads (approximately 79 percent) in the cloud. Additionally, 84 percent of enterprises and 61 percent of small-medium businesses have a *multicloud* strategy leveraging an average of nearly 5 public and/or private clouds.[2] Similarly, the Enterprise Strategy Group found that production server workloads increasingly run on a mix of cloud-ready architectures, including *virtual machines* (34 percent), *containers* (23 percent), and *serverless* (15 percent).[3]

Consumerization. The process of consumerization occurs as end users increasingly find personal technology and apps that are more powerful or capable, more convenient, less expensive, quicker to install, and easier to use than enterprise IT solutions.

Bring your own device (BYOD). Closely related to consumerization is BYOD, a policy trend in which organizations permit end users to use their own personal devices, primarily smartphones and tablets, for work-related purposes. BYOD relieves organizations from the cost of providing equipment to employees but creates a management challenge because of the vast number and type of devices that must be supported.

Bring your own apps (BYOA). Web 2.0 apps on personal devices are increasingly being used for work-related purposes. As the boundary between work and personal lives becomes less distinct, end users are practically demanding that these same apps be available to them in their workplaces.

Mobile computing. The appetite for rapid, on-demand access to apps and data from anywhere, at any time, on any device is insatiable. There are now more than 8 billion mobile subscriptions worldwide, and total mobile monthly data traffic (including audio, file sharing, social networking, software uploads and downloads, video, web browsing, and other sources) is about 40 exabytes![4]

5G cellular wireless. Each new generation of wireless connectivity has driven a wealth of new innovations, and the move to the fifth-generation of cellular wireless (5G) is well underway, with mobile network operators announcing 5G pilot trials and commercialization plans as they expand their geographic footprints. The latest 5G applications are consumer-driven, help governments implement 5G for smart city rollouts, and bring 5G service experience to the public by seamlessly covering major sports events, among others.

[2] RightScale 2019 State of the Cloud Report from Flexera." February 27, 2019. https://www.flexera.com/2019-cloud-report.

[3] Cahill, Doug. "Leveraging DevSecOps to Secure Cloud-native Applications." Enterprise Strategy Group. December 9, 2019. https://www.esg-global.com/research/esg-master-survey-results-leveraging-devsecops-to-secure-cloud-native-applications.

[4] "Ericsson Mobility Report, November 2019." Ericsson. November 2019. https://www.ericsson.com/en/mobility-report/reports/november-2019.

The promise of intelligent connectivity will drive massive adoption of the internet of things (IoT) and has the potential to transform industries as well. We're now talking about the Enterprise of Things – networked industrial devices, sensors, networks and apps that connect businesses. As today's enterprises undergo digital transformation, they'll be looking for 5G networks to drive true Industry 4.0 transformation, leveraging automation, *artificial intelligence* (AI), and IoT.

Content delivery networks (CDN). Enterprises are using *content delivery networks* (CDNs) like Akamai, Amazon CloudFront, and Limelight networks to distribute their web products and services to customers worldwide. CDNs will grow even more prominent as 5G adoption continues to expand.

Key Terms

Public cloud is a cloud computing deployment model that consists of a cloud infrastructure that is open to use by the general public.

Private cloud is a cloud computing model that consists of a cloud infrastructure that is used exclusively by a single organization.

Multicloud is an enterprise cloud environment (or strategy) consisting of two or more public and/or private clouds.

A *virtual machine* (VM) is an emulation of a physical (hardware) computer system, including CPU, memory, disk, operating system, and network interfaces.

A *container* is a standardized, executable, and lightweight software code package that contains all the necessary components to run a given application (or applications) – including code, runtime, system tools and libraries, and configuration settings – in an isolated and virtualized environment to enable agility and portability of the application workloads.

Serverless generally refers to an operational model in cloud computing in which applications rely on managed services that abstract away the need to manage, patch, and secure infrastructure and virtual machines. Serverless applications rely on a combination of managed cloud services and function-as-a-service (FaaS) offerings.

Artificial intelligence (AI) is the ability of a system or application to interact with and learn from its environment, and to automatically perform actions accordingly, without requiring explicit programming.

A *content delivery network* (CDN) is a network of distributed servers that distributes cached webpages and other static content to a user from a geographic location that is physically closest to the user.

Web 3.0, as defined on ExpertSystem.com, is characterized by the following five characteristics: semantic web, artificial intelligence, 3D graphics, connectivity, and ubiquity.

Moving beyond Web 2.0, *Web 3.0* will transform the enterprise computing landscape over the next decade and beyond. Web 3.0, as defined on ExpertSystem.com, is characterized by five main features:

Semantic web. “The semantic web improves web technologies in order to generate, share and connect through search and analysis based on the ability to understand the meaning of words, rather than on keywords and numbers.”

Artificial intelligence. “Computers can understand information like humans in order to provide faster and more relevant results.”

3D graphics. 3D design is “used extensively in websites and services.”

Connectivity. “Information is more connected thanks to semantic metadata. As a result, the user experience evolves to another level of connectivity that leverages all the available information.”

Ubiquity. “Content is accessible by multiple applications, every device is connected to the web, [and] the services can be used everywhere.”[5]

For many, the vision of Web 3.0 is to return the power of the internet to individual users, in much the same way that the original Web 1.0 was envisioned. To some extent, Web 2.0 has become shaped and characterized, if not controlled, by governments and large corporations dictating the content that is made available to individuals and raising many concerns about individual security, privacy, and liberty. Specific technologies that are evolving and beginning to form the foundations of Web 3.0 include (among others):

AI and *machine learning* are two related technologies that enable systems to understand and act on information in much the same way that a human might use information. AI acquires and applies knowledge to find the most optimal solution, decision, or course of action. Machine learning is a subset of AI that applies algorithms to large datasets to discover common patterns in the data that can then be used to improve the performance of the system.

Blockchain is essentially a data structure containing transactional records (stored as blocks) that ensures security and transparency through a vast, decentralized peer-to-peer network with no single controlling authority. *Cryptocurrency*, such as Bitcoin, is an example of a blockchain application.

Data mining enables patterns to be discovered in large datasets by using machine learning, statistical analysis, and database technologies.

[5] Expert System. 2017. “5 main features of Web 3.0.” Accessed June 3, 2018. http://www.expertsystem.com/web-3-0/.

Mixed reality includes technologies, such as *virtual reality* (VR), *augmented reality* (AR), and *extended reality* (XR), that deliver an immersive and interactive physical and digital sensory experience in real time.

Natural language search is the ability to understand human spoken language and context, rather than a *Boolean* search, for example, to find information.

Key Terms

Machine learning is a subset of AI that applies algorithms to large datasets to discover common patterns in the data that can then be used to improve the performance of the system.

Blockchain is essentially a data structure containing transactional records (stored as blocks) that ensures security and transparency through a vast, decentralized peer-to-peer network with no single controlling authority. Cryptocurrency is an internet-based financial instrument that uses blockchain technology.

Data mining enables patterns to be discovered in large datasets by using machine learning, statistical analysis, and database technologies.

Mixed reality (MR) includes technologies, such as virtual reality (VR), augmented reality (AR), and extended reality (XR), that deliver an immersive and interactive physical and digital sensory experience in real time. *Virtual reality* is a simulated experience. *Augmented reality* enhances a real-world environment with virtual objects. *Extended reality* broadly covers the spectrum from physical to virtual reality with various degrees of partial sensory to fully immersive experiences.

Natural language search is the ability to understand human spoken language and context, rather than a Boolean search, for example, to find information. *Boolean* refers to a system of algebraic notation used to represent logical propositions.

Organizations are often unsure of the potential business benefits – and the inherent risks – of new trends such as Web 2.0 and Web 3.0, and therefore either:

Implicitly allow personal technologies and apps by simply ignoring their use in the workplace, or

Explicitly prohibit their use but are then unable to effectively enforce such policies with traditional firewalls and security technologies

Whether personal technologies and apps are implicitly allowed (and ignored) or explicitly prohibited (but not enforced), the adverse results of ineffective policies include:

Lost productivity because users must either find ways to integrate these unsupported technologies and apps (when allowed) with the enterprise infrastructure or use applications that are unfamiliar to them or less efficient (when personal technologies and apps are prohibited)

Potential disruption of critical business operations because of underground or back-channel processes that are used to accomplish specific workflow tasks or to circumvent controls, and are known to only a few users and are fully dependent on their use of personal technologies and apps

Exposure to additional risks for the enterprise due to unknown – and therefore unpatched – vulnerabilities in personal technologies and apps, and a perpetual cat-and-mouse game between employees who circumvent controls (for example, with external proxies, encrypted tunnels, and remote desktop applications) and security teams that manage these risks

Penalties for regulatory non-compliance, for example, the EU General Data Protection Regulation (GDPR), the U.S. Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS)

As these trends continue to blur the distinction between the internet and the enterprise network, new security challenges and risks emerge, including:

New application threat vectors

Turbulence in the cloud

SaaS application risks

New application threat vectors

Exploiting vulnerabilities in core business applications has long been a predominant attack vector, but threat actors are constantly developing new tactics, techniques, and procedures (TTPs). To effectively protect their networks and cloud environments, enterprise security teams must not only manage the risks associated with a relatively limited, known set of core applications but also the risks associated with an ever-increasing number of known and unknown cloud-based applications. The cloud-based application consumption model has revolutionized the way organizations do business, and applications such as Microsoft Office 365 and Salesforce are being consumed and updated entirely in the cloud.

Classifying applications as either “good” (allowed) or “bad” (blocked) in a clear and consistent manner has also become increasingly difficult. Many applications are clearly good (low risk, high reward) or clearly bad (high risk, low reward), but most are somewhere in between – depending on how the application is being used.

For example, many organizations use social networking applications such as Facebook for important business functions such as recruiting, research and development, marketing, and consumer advocacy. However, these same applications can be used to leak sensitive information or cause damage to an organization’s public image – whether inadvertently or maliciously.

Many applications are designed to circumvent traditional port-based firewalls (discussed in Section 2.3.1), so that they can be easily installed and accessed on any device, anywhere and anytime, using techniques such as:

Port hopping, in which ports and protocols are randomly changed during a session.

- **Use of non-standard ports**, such as running Yahoo! Messenger over TCP port 80 (HTTP) instead of the standard TCP port for Yahoo! Messenger (5050).
- **Tunneling within commonly used services**, such as when peer-to-peer (P2P) file sharing or an instant messenger (IM) client such as Meebo is running over HTTP.
- **Hiding within SSL encryption**, which masks the application traffic, for example, over TCP port 443 (HTTPS). More than half of all web traffic is now encrypted.

Many traditional client-server business applications are also being redesigned for web use and employ these same techniques for ease of operation while minimizing disruptions. For example, both *remote procedure call* (RPC) and Microsoft SharePoint use port hopping because it is critical to how the protocol or application (respectively) functions, rather than as a means to evade detection or enhance accessibility.

Key Terms

Remote procedure call (RPC) is an inter-process communication (IPC) protocol that enables an application to be run on a different computer or network, rather than the local computer on which it is installed.

Applications can also be hijacked and repurposed by malicious actors, such as was done in the 2014 Heartbleed attack. According to an April 2014 Palo Alto Networks article:

“[T]he story of Heartbleed’s impact has been focused on the compromise of HTTPS-enabled websites and web applications, such as Yahoo!, Google, Dropbox, Facebook, online banking, and the thousands of other vulnerable targets on the web. These are of huge impact, but those sites will all be updated quickly….

“For security professionals, [the initial Heartbleed attack] is only the tip of the iceberg. The vulnerability puts the tools once reserved for truly advanced threats into the hands of the average attacker – notably, the ability to breach organizations, and move laterally within them. Most enterprises of even moderate size do not have a good handle on what services they are running internally using SSL encryption. Without this baseline knowledge, it is extremely difficult for security teams to harden their internal attack surface against the credential and data stealing tools Heartbleed enables. All footholds for the attacker with an enterprise network are suddenly of equal value.”[6]

As new applications are increasingly web-enabled and browser-based, HTTP and HTTPS now account for about two-thirds of all enterprise network traffic. Traditional port-based firewalls and other security infrastructure cannot distinguish whether these applications, riding on HTTP and HTTPS, are being used for legitimate business purposes. Thus, applications (including malware) have become the predominant attack vector to infiltrate networks and systems.

[6] Simkin, Scott. “Real-world Impact of Heartbleed (CVE-2014-0160): The Web is Just the Start.” Palo Alto Networks. April 2014. https://researchcenter.paloaltonetworks.com/2014/04/real-world-impact-heartbleed-cve-2014-0160-web-just-start.