# TABLE OF CONTENTS

Analytics and Data Management, Business Intelligence, and Data Warehousing ............. 1  
Application and Business Services .................................................................................. 2  
Application Development and Management .................................................................... 5  
Endpoint and Identity Management .................................................................................. 6  
Hybrid Cloud, Software-Defined Infrastructure, and Machine Learning ......................... 9  
Intelligent Automation ....................................................................................................... 11  
Network Management ....................................................................................................... 12  
Security and Risk Management ......................................................................................... 14
With all of the hype around artificial intelligence (AI) and machine learning (ML), it is difficult to understand what is real and what is being overstated. There has also been a proliferation of money invested and new vendors launching AI and ML products. This research is designed to help business leaders discern what is real and what is just hype for AI and ML. In addition, it will align specific business requirements with each segment of the complex AI and ML market.

As the move to the cloud for analytics accelerates, data management (to the risk of failure) continues to grow. This research will identify trends, best practices, and recommendations to mitigate risk for cloud migrations and help insight-driven organizations maximize their ROI for cloud investments.

Leading organizations have taken major strides toward the proliferation of insight-driven decisions, but as the market continues to grow, new categories and new entrants have made it difficult to identify the right solution for each unique set of business drivers. This research is designed to help business leaders differentiate the many different paths to smart decisions for their organizations. In addition, it will align specific business requirements with each segment of the complex BI, analytics, and AI markets.

Most definitions of digital marketing (DM) focus on digital interaction with customers or prospects via mobile or connected devices and apps. However, as DM matures, it is no longer focused on the device or the app: it is all about the data. Experienced digital marketers are using marketing content and engagement on digital channels to reach new customers and to collect data that generates insight for the continuous improvement of marketing ROI. The combination of analytics, artificial intelligence, and automation holds the keys to creating significant differentiation and value. This research digs into understanding best practices, technology, and analytics needed to outpace the competition and drive the continuous process of marketing improvement in a digital world.
APPLICATION AND BUSINESS SERVICES
BY DENNIS DROGSETH AND VALERIE O’CONNELL

Enterprise Service Management (ESM) and the ITSM Landscape
Quarter 1, 2020
VALERIE O’CONNELL

EMA research shows that 87% of organizations have some level of ESM deployment from their ITSM platform/team. What’s more, given a healthy selection of possible responses, 38% rated the impact of supporting ESM as “transformational” on the relationship between IT and business stakeholders. Although potentially game-changing, these advances are not free of challenge. The technological complexity of advances in AI and automation, functional understanding, budget prioritization, and organizational resistance all play a role in adoption. Designed to benefit both vendors and ESM/ITSM practitioners, this research drills down into the details of implementation, including:

• Characteristics of ITSM platforms that either facilitate or complicate ESM
• Functionality and technologies that invigorate new initiatives
• Practical matters of policies, politics, and people
• Use cases most likely to return high rates of reward
• Predictable challenges, drivers, and benefits realized

A Holistic Look at How Automation is Transforming IT for the Digital Age: Technologies, Politics, and Processes
Quarter 1, 2020
DENNIS DROGSETH/DAN TWING

To say that automation is popular is now an understatement. Beyond that, what’s really meant by automation—along with how it serves IT—tends to remain a parochial discussion based on market-defined boxes and vendor marketing priorities. This research will examine automation adoptions holistically, breaking down every relevant market wall, to create a unique “geographical” map of automation technologies in play: how they’re used, and where the gaps are. It will also examine how AI/ML and automation are coming together—where, how, and why? The research will explore the human handshake with automation in terms of processes, politics, organizational models, best practices, and even psychology. How can automation be viewed as augmenting human potential rather than displacing it? Finally, the research will provide guidelines for effective automation adoption across various use cases and strategic initiatives in support of both IT and business transformation.
At the intersection of IT and running the business, ITSM both facilitates and is facilitated by innovations in AI and automation. Far from shrinking the ITSM organizational footprint, these advances increasingly extend ITSM’s reach into and across the enterprise. Recent EMA research shows that more than half of organizations across industries plan substantial growth in ITSM over the next three years with budget increases to match, and only 2% anticipating a decline.

This research will examine the ways that organizations keep pace with growing demand for ITSM services and support. Looking first to determine high-demand areas, it will probe steps commonly taken to refresh—and even revolutionize—platforms, people, processes, and policies already in place. It will explore the rich ecosystem of products, technologies, and services designed to build upon ITSM platforms and make modernizing or upgrading ITSM an attractive alternative to replacement.

The high-tech world has finally awoken to the powerful realities of AIOps and IT analytics, which can more broadly bring surprising values across a wide variety of outcomes. Once data is collected dynamically and effectively, it can potentially be applied to various use cases with what EMA has already seen as proven, and sometimes they have dramatic benefits.

However, the specifics of relating AIOps investments to given use cases, along with effective deployment strategies, still too often remain a mystery. This radar is designed to provide IT executive and technical buyers with a clear, functional roadmap of the AIOps and IT analytics vendors in 2020 so they can shop with nonlinear, multidimensional insights while seeking the technology that’s best for them.

This radar will build on extensive EMA research on AIOps, including “AIOps and IT Analytics at the Crossroads” (October 2018), to review vendor strengths across three critical use cases:

- **Performance and availability**: This is the core AIOps value proposition, and a foundation that not only ensures that IT services perform consistently and effectively, but also unites IT organizations across silos with shared data and proactive insights.

- **Change management/cloud migration**: With dynamic, performance-aware data, AIOps and IT analytics vendors can provide significant insights into change impacts across the traditional legacy landscape, as well as hybrid and multi-cloud. Insights here can also help to support improved DevOps performance and cost optimization in cloud migrations.

- **Business alignment/business outcomes**: Having a dynamic system of record on performance and change can become an even richer value when these insights are effectively linked to business outcomes, from revenue to OpEx efficiencies to business process impacts, among others.
Digital Experience Management: Where Service and Business Performance Come Together
Quarter 3, 2020
DENNIS DROGSETH/VALERIE O’CONNELL

We will build creatively upon EMA’s extensive history in researching user and customer experience management in all its dimensions. The goal is to look at the critical handshakes in 2020 that make end-user experience management (EUEM) a transformative investment in unifying IT decision-making and aligning it more effectively with the business overall. Some of the handshakes EMA will focus on include:

- **IT service management (ITSM) to operations**: To what degree are IT organizations seeking to integrate insights in terms of user behaviors, requests, and issues with IT operations transactional and other data?
- **DevOps initiatives**: How is EUEM being used in 2020 to inform on DevOps initiatives to unify development and operations teams across the full application lifecycle?
- **IT and business alignment**: How and in what way is the business view of EUEM changing? To what degree is EUEM data being applied to support business planning for critical new application requirements, including insights on usage, value, and outcomes? What's needed and what's lacking?
- **Legacy to cloud**: How is EUEM data being used to support requirements for cloud migration and cloud optimization?

The SecOps Handshake from Both Sides of the Equation
Quarter 4, 2020
DENNIS DROGSETH/PAULA MUSICH

This research will build on EMA's groundbreaking 2017 study, "SecOps: Integrating Security for Performance, Asset Optimization, and Change Management—Two Views" in providing a clear 2020 roadmap of how security and operations are (or are not) progressing in working together more effectively in a variety of use cases, including the increasingly critical requirements of digital transformation. More specifically, these will include:

- Shifting role relationships, priorities, technology options, and shared metrics between security (cyber detection, risk/compliance, and fraud) and operations, development, and IT service management (ITSM) teams
- Obstacles and benefits along the way
- Impacts of changing requirements given cloud, agile/DevOps, mobile, digital transformation, and other trends
- Technologies that are leading in unifying SecOps initiatives and improving SecOps’ overall effectiveness as viewed from both sides (security and operations)
## Application Development and Management

**BY STEPHEN HENDRICK**

<table>
<thead>
<tr>
<th>Study Title</th>
<th>Quarter</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>What Enterprises Expect from AI and ML Technologies</td>
<td>Quarter 1, 2020</td>
<td>AI and ML are buzzwords that every vendor has woven into their IT vocabulary and elevator pitch. What are enterprise expectations around AI and ML, and how have these technologies been influencing and impacting how enterprises steer business and IT activities? This study will look at AI and ML from current state and future state perspectives, evaluate the technologies and tools in use, and how effectively vendors have been able to address enterprise needs.</td>
</tr>
<tr>
<td>What it Means to be a Data-Driven Enterprise</td>
<td>Quarter 2, 2020</td>
<td>Most apps developed over the last 20 years have been scheduled (batch) or reactive (query and response) and focused on either informational and/or transactional. Modern application development brings EDA, which enables an enterprise to be formally data-driven. Data-driven application development now means that enterprises can intelligently react in real time to events that are occurring and proactively take actions relative to a threat or opportunity. Analytics is a big part of the data-driven story since real-time analysis is needed to determine how exactly to optimize and how to respond to a threat or opportunity. This research will focus on data-driven enterprises and the challenges, benefits, utility, tools, changes to IT, and the business models that have followed. EMA can also run this survey against non-data-driven enterprises and look for how different their responses are. This report should appeal to vendors that do data streaming, event management, rules, and analytics.</td>
</tr>
<tr>
<td>Shifting All the Way Left with DevOps</td>
<td>Quarter 4, 2020</td>
<td>The premise is that good code requires good planning. Today, DevOps has zeroed in on the pipeline, which is focused on CI/CD writing/testing/releasing code. I’ve already looked at the intersection of Development and Ops, but no one is providing a voice to the myriad of products that lay the foundation for a successful and efficient journey through the pipeline. This survey will look at pre-pipeline activities including design, architecture, requirements, IT-PPM, and test management tools and will find out what enterprises are doing in this primary market, best practices, tool use, problems, needs, strategy, maturity, etc.</td>
</tr>
</tbody>
</table>
**ENDPOINT AND IDENTITY MANAGEMENT**  
**BY STEVE BRASSEN**

### EMA Top 3 Report: Ten Priorities for Enabling Secure Access in 2020  
**Quarter 1, 2020**

Enterprises productivity, profitability, and success in meeting business objectives are dependent on the ability of workforces to access and utilize the applications, data, emails, and other IT services necessary to complete job tasks. However, increased pressures to enable workforce mobility and the distribution of IT services across a variety of public and private hosting environments have challenged organizations to grant secure and reliable access to those resources. This Enterprise Management Associates (EMA) decision guide is intended to provide actionable advice on the best practices and solutions organizations should adopt to empower end-user productivity while minimizing risk profiles. For each of the ten priorities noted by surveyed organizations, EMA will identify the top three leading providers offering solutions in the market in 2020.

### Establishing Trust in a Zero Trust World  
**Quarter 1, 2020**

Recognizing that defining traditional security boundaries can no longer be relied on as an effective method for securing enterprise applications, data, and IT services, organizations are broadly embracing Zero Trust approaches to access controls. In a world dependent on mobile workforces, hybrid cloud architectures, and complex network topologies, no access connections should inherently be trusted and permitted without some level of authentication and authorization. Unfortunately, while the term "Zero Trust" has resonated with the enterprise security market, there are no established guidelines to identify which characteristics would qualify an identity and access management (IAM) platform to be considered a Zero Trust solution. To help bring clarity to this designation, EMA will conduct survey-based research to determine the most essential requirements and challenges that should be addressed by a Zero Trust solution, as well as the key features and best practices that should be adopted to positively establish trust when enabling access to enterprise IT resources.
<table>
<thead>
<tr>
<th>The Intelligent Workspace: Using Intelligence Technologies to Enhance User Experiences, Service Delivery, and Access Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarter 2, 2020</td>
</tr>
</tbody>
</table>

Traditional processes for endpoint management simplify administrative practices by standardizing how end users provision, configure, and utilize IT services. However, user requirements and security considerations can radically differ between users under varying circumstances. For instance, where the user is physically located, the device they are using, the network they are communicating over, and the types of IT resources they are accessing all contribute to the contextual element that needs to be considered when providing a digital workspace that will optimally enable user effectiveness and security assurance. By injecting intelligence technologies—such as analytics, cognitive computing, machine learning, and language processing—into workspace environments, organizations can enable dynamic environments that adapt to changing user requirements, rather than forcing users to adapt to IT requirements. In this research project, EMA will survey organizations to provide actionable guidance on the value of intelligence technologies in digital workspace environments, including how the different approaches can enhance security, reduce management efforts and related costs, and boost workforce productivity.

<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarter 3, 2020</td>
</tr>
</tbody>
</table>

While there is a growing recognition of the need to enforce stronger access controls around the use of privileged accounts, the majority of enterprises continue to rely on legacy processes that only enforce security at the time of authentication. Because of the superlative permissions granted to privileged accounts, it is insufficient to rely on a single authentication control, such as a password, as a means of granting unfettered access to the most sensitive IT assets. To ensure continuous compliance with business, security, and regulatory commitments, organizations should implement solutions that monitor privileged activities and provide dynamic alerts and protections in real-time. EMA’s survey-based research is intended to quantify the value of a real-time protection approach to privileged access management. Respondents will provide indications of the security risks inherent in traditional, authentication-only approaches, as well as optimal approaches to enabling real-time protections of privileged accounts.
<table>
<thead>
<tr>
<th>Study Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Credential Loss and Recovery</strong></td>
<td>Identity management processes are most frequently dependent on the ability of users to memorize or otherwise retain credential information, such as passwords or PINs. Unfortunately, fallible humans can forget or misplace credential information or may inadvertently be locked out of online accounts, such as by repeated failed login attempts. Typical account recovery processes are extremely high-friction and can have profound impacts on end-user productivity and access experiences. Additionally, EMA primary research has indicated that administrative efforts to assist users with credential recovery are the most time-consuming identity and access management tasks performed by enterprise IT operations teams. In this research project, EMA will conduct a survey of organizations across a variety of industry horizontals and verticals to determine the frequency and consequences of credential losses, as well as to determine the optimal approaches for reducing incidents of credential loss. Also, the research will evaluate the most effective methods for recovering lost credentials that ensure stringent security requirements are maintained while minimizing end-user efforts.</td>
</tr>
<tr>
<td><strong>Customer Identity and Access Management (CIAM): Responsible Solutions for Creating Positive Consumer Experiences</strong></td>
<td>Today’s modern businesses are dependent on managing customer accounts to support sales transactions, information gathering, customer service, technical support, and other consumer interactions. Customer experiences with accessing these accounts can have a profound effect on business success since consumers often migrate to competitors that offer lower-friction access experiences. At the same time, it is essential that strong security controls protect customer information and intellectual property. To assist organizations in the identification of optimal approaches to CIAM that balance security with low-friction experiences, EMA will conduct a survey of consumer-focused businesses to determine which technologies and practices provide the greatest advantages to customer satisfaction. Additionally, the research will seek to quantify the business costs of poor CIAM implementations, as well as the direct business benefits that can be achieved through the adoption of more effective approaches.</td>
</tr>
</tbody>
</table>
HYBRID CLOUD, SOFTWARE-DEFINED INFRASTRUCTURE, AND MACHINE LEARNING
BY TORSTEN VOLK

Five Critical Rules for Optimizing Infrastructure for App Development, Data Management, Business Analytics, and AI
Quarter 1, 2020

This research will reveal the five critical rules for optimizing servers, storage, and network infrastructure in the data center and cloud for continuous application delivery, federated data governance and management, business analytics, artificial intelligence (AI), and further modern use cases. Based on EMA's big data analytics-driven approach to end-user research, the study will look at pain points, processes, and technology adoption patterns of a large number of real-life enterprise projects to enable readers to learn from the successes and failures of their peers.

Five Best Practices for Optimizing DevOps and ITOps Through Machine Learning, Deep Learning, and AI
Quarter 1, 2020

First, this study will pinpoint the critical DevOps and ITOps pain points experienced by modern enterprises of different sizes and verticals, based on EMA's own big data-driven approach toward end-user research. The report will then outline how machine learning, deep learning, and AI-driven functions, processes, and tools can be used to address the previously identified DevOps and ITOps challenges.

Five Best Practices for Achieving Continuous Security and Compliance for Dev and Ops
Quarter 1, 2020

CIOs identify continuous security and compliance as the most significant hurdles preventing their organizations from releasing software capabilities at the desired pace, efficiency, and quality. This end-user research report reveals five best practices enabling DevOps and IT operations to eliminate the key pitfalls that prevent them from achieving a state in which security and compliance are baked into the continuous release process, and where they can produce audit reports through the push of a button.

Quarter 2, 2020

This EMA Top 3 Enterprise Decision Guide identifies the three most innovative software products in a number of different categories that are all aimed at making multi-cloud, hybrid cloud, and Kubernetes environments suitable for mission-critical applications. The report will be based on end-user data gathered from approximately 1,000 real-life enterprise projects and drill into challenges related to the availability, performance, compliance, security, and operations costs of modern application environments.

EMA Top 3 Enterprise Decision Guide for Infrastructure as Code Platforms
Quarter 2, 2020

The rise of Kubernetes, fueled by business units pushing for increasingly frequent, granular, high-quality, and cost-effective software releases, makes the adoption of infrastructure as code solutions mandatory. This EMA Top 3 Enterprise Decision Guide identifies the top products making infrastructure as code accessible across modern enterprises leveraging different data center and cloud infrastructure, and following a more and more hybrid application architecture paradigm. Readers will benefit from experiences gained through the analysis of approximately 1,000 real-life enterprise projects leveraging infrastructure as code for different use cases and within a broad range of fundamentally different application architectures.
<table>
<thead>
<tr>
<th>Title</th>
<th>Quarter</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hyperconverged Infrastructure for Multi-Cloud, Hybrid Cloud, and Edge</strong></td>
<td>3, 2020</td>
</tr>
<tr>
<td>Modern hyperconverged infrastructure (HCI) provides a consistent compute, storage, and networking foundation for cloud in the data center, the public cloud, and at the edge. This EMA big data-driven research project explores the current level of adoption of hyperconverged systems for each one of these use cases in the light of today’s enterprise pain points and the resulting investment priorities. The report will answer questions like, “What are the key characteristics of HCI that make it suitable for my specific use case?” and “Should I look at AWS Outpost or Azure Stack in addition to or instead of HCI platforms from traditional vendors, such as Cisco, Dell EMC, Nutanix, HPE, IBM, VMware, or Red Hat?” The report will be based on a large number of customer opinions and real-life projects to derive a “checklist” for the individual types of enterprise customers to consider when making purchasing decisions.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Quarter</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Changing Job Requirements for Developers and Operators in 2020 and Beyond</strong></td>
<td>4, 2020</td>
</tr>
<tr>
<td>This research looks at real-life experiences and opinions from approximately 1,000 IT professionals and software developers in terms of what new skills, soft and hard, they believe they will have to acquire today and in the near future. This will reflect requirements derived from the concerted push of many IT organizations to turn into a strategic asset and part of the corporate value chain, while leaving their old “cost center smell” behind. The report will illustrate where IT operators, developers, and executives currently are in this development process and where they are planning to go next. Readers will also learn from hiring practices that worked and did not work for different sizes and types of organizations.</td>
<td></td>
</tr>
</tbody>
</table>
# Intelligent Automation

**BY DAN TWING**

## A Holistic Look at How Automation is Transforming IT for the Digital Age: Technologies, Politics, and Processes

*Quarter 1, 2020*

DAN TWING/DENNIS DROGSETH

To say that automation is popular is now an understatement. Beyond that, what's really meant by automation—along with how it serves IT—tends to remain a parochial discussion based on market-defined boxes and vendor marketing priorities. This research will examine automation adoptions holistically, breaking down every relevant market wall, to create a unique “geographical” map of automation technologies in play: how they’re used, and where the gaps are. It will also examine how AI/ML and automation are coming together—where, how, and why? The research will explore the human handshake with automation in terms of processes, politics, organizational models, best practices, and even psychology. How can automation be viewed as augmenting human potential rather than displacing it? Finally, the research will provide guidelines for effective automation adoption across various use cases and strategic initiatives in support of both IT and business transformation.

## The Human Element in Workload Automation: Organizational Structures and Best Practices to Evangelize Automation Across the Enterprise

*Quarter 2, 2020*

This research will focus on two primary areas. First, it will look at the various ways organizations organize scheduling teams and manage workload automation software. Many are centralized, with only a limited team defining jobs. Others have a core team to set naming standards and best practices, and help train broader teams of operations, developers, and even business users to monitor, launch, and define jobs. This part of the research will look at various means of organizing teams, benefits, and problems, and how well automation is used and spread across the enterprise. The second focus will be corporate culture toward automation, the role of the automation team in broader IT operations and business process automation, and what makes some companies super successful with automation. Usually, an evangelist-type scheduling leader can expand the use of a good WLA tool and inspire its use for much broader automation across IT operations and into business processes. EMA believes only about 5% of user organizations achieve this level of success and impact with WLA software. This research will attempt to understand what sets these organizations apart and how to replicate it so more customers can benefit from automation evangelism around WLA software.
**Network Management Megatrends 2020: NetSecOps, Hybrid Cloud, and More**
Quarter 1, 2020

EMA’s biannual Network Management Megatrends research examines how new technologies and business initiatives affect and transform enterprise network management tools and practices. EMA has been publishing this research since 2008, making it the benchmark for the network management industry. The Megatrends report tracks changes in network management tool requirements, challenges, and priorities. Megatrends that will be explored in 2020 will include collaboration between network operations and security operations, data center SDN and hybrid cloud, and the Internet of Things.

**Application Delivery Controllers for Multi-Cloud Enterprises**
Quarter 2, 2020

Enterprise cloud adoption has disrupted the Layer 4-7 networking world. Monolithic, appliance-based load balancers and application delivery controllers no longer meet the requirements of the modern application team. Hybrid cloud and multi-cloud architectures require ADC solutions characterized by lightweight software, automation, and analytics. Microservices, containers, service mesh, and more are driving change and forcing vendors to diversify their offerings. This research will reveal how ADC buyers are shifting their approach to Layer 4-7 networking within legacy data center and modern, cloud-native environments.

**Zero Trust Network Architecture Strategies: Microsegmentation, Software-Defined Perimeters, and Beyond**
Quarter 2, 2020

The network perimeter was never 100% secure, but today that perimeter is essentially gone. Enterprises deploy critical applications and assets into public cloud environments every day. The Internet of Things is proliferating, causing the network edge to get fuzzier and more diverse. Network architects need a Zero Trust approach to networking. This research will look at how the network team supports this shift toward deperimeterization. We will examine emerging enterprise requirements and strategies around microsegmentation, software-defined perimeters, and other network technologies that control network access in digital enterprises.

**AIOps and Network Management: Enriching NetOps Tools with Analytics**
Quarter 3, 2020

Many network infrastructure and network management tool vendors are investing millions in developing AIOps technology, particularly machine learning algorithms, that enhance the value of their existing product portfolios. Network managers are leveraging these technologies for anomaly detection, automated root-cause analysis, and guided remediation. As vendors introduce new analytics features, network managers will need help navigating these new capabilities. They need to know exactly what they can expect from such technologies. Meanwhile, vendors need to know how to deliver these technologies in a way that is consumable and useful. They need to answer one fundamental question: Will our customers pay for this? This EMA research will define the future of AIOps in the network management industry.
SD-WAN solutions have ushered in an era of unprecedented WAN transformation, as enterprises strive for networks that are more secure, cloud-enabled, and agile. EMA’s biennial research on WAN transformation goes beyond SD-WAN adoption rates and looks at how enterprises derive value from these investments. This research will look at how enterprises are using SD-WAN and related technologies, such as network virtualization, cloud-based security services, and internet connectivity, to turn their networks into platforms for a digital future.

EMA research found that network performance management (NPM) is more a mission than a platform. Enterprises rarely have a single, unified NPM solution. Instead, they use a handful of tools to support their NPM requirements and to address their NPM use cases. This EMA Radar will perform separate evaluations of two general classes of NPM vendors: vendors that primarily collect and analyze infrastructure metrics (e.g., via SNMP MIBs/traps, device APIs) and vendors that collect and analyze production network traffic (packets, packet metadata, network flow records, etc.).

Using primary research, this EMA Radar will assess the core capabilities and features that address central NPM use cases, including operational monitoring, troubleshooting, and capacity planning. It will also examine the overall practitioner experience in procuring, deploying, administering, and using specific NPM products.
Death of the Penetration Tester: How Automated Application and Environment Testing are Changing the Testing Game
Quarter 1, 2020
AUTHOR: EMA ANALYST

Penetration testing has been around since the 1990s, but nothing much changed until the last few years. Talented people with their own cadre of tools, being engaged somewhere between annually and quarterly at significant expense, tried to find their way into systems to help identify flaws in software and controls weaknesses so they can be addressed. The testing is often fraught with issues and incidents of poorly maintained or out-of-date systems failing due to various tests posted against them, causing negative business impacts.

In the last three years, a new branch of attack simulation technologies sprung up to not only automate much of this previously manually-driven process, but to be able to provide insights on a nearly continuous basis with no threat to the operational environment.

EMA research questions IT and security professionals, as well as customers of solutions providers, to learn how organizations are taking advantage of this new opportunity to overcome challenges of traditional penetration testing and receiving better results faster to close the window of opportunity for attackers.

Using IT Security Orchestration and Automation to Combat the IT Security Skills Gap: How Security Vendors are Helping
Quarter 1, 2020
PAULA MUSICH

The IT security skills shortage is not going away anytime soon. With estimates that 3.5 million cybersecurity jobs will go unfilled by 2021, the need for better automation of repetitive functions and other workflow streamlining efforts has never been greater. The good news is that startups and established security vendors alike are stepping up to address the problem with increasing levels of integration, automation, and collaboration enhancements. Are security orchestration and automation tools making a dent in the productivity issue? What are the different methods being applied to the problem of security analyst productivity? Are customers realizing a significant increase in productivity and process accuracy? Which integrations or techniques are having the biggest positive and negative impacts? Are organizations ready to take the next step to automate their processes and procedures, or will all of the automation just get them to negative outcomes faster? This EMA study will seek to answer such questions and illustrate how customers can gain ground on the problem.
OT, IoT, What the…!? Why IoT is More Than a Nuisance Threat and What to do About it

Quarter 1, 2020
AUTHOR: EMA ANALYST

The Internet of Things, consumer, commercial, and industrial sensors and controllers are growing at a nearly exponential rate. Whether you know you have devices in your network or not, they are probably there. Consumer IoT offers beachheads for intrusion, data exfiltration, and privacy invasion, and works as a platform for bot nets. Commercial IoT can be compromised for the same ends, with the addition of damaging or destroying inventory to cause business losses. Industrial IoT, often referred to as operational technology (OT), has all of the issues of consumer and commercial IoT with the added threat of loss of human life.

In this EMA research, learn the perspectives of business personnel versus security personnel and the difference in perspective by dissimilar industries on the threats of IoT to business privacy, operations, and resiliency. Understand the IoT threats being experienced versus what has little or no factual basis and what’s being used to spread fear, uncertainty, and doubt (FUD). The research will also examine what organizations are using to identify IoT in their environments and to manage the relevant threats and risk.

Ransomware Attacks: How Not to be a Victim

Quarter 2, 2020
PAULA MUSICH

Ransomware continues to be one of the top threats to organizations, with attackers now especially focused on the less-protected SME segment, state and municipal governments, and any organization still using outdated and unpatched Windows 7 systems. More often than not, the latter are used in manufacturing, healthcare, education, and government, and they are often deemed mission-critical, providing fertile hunting ground for attackers. Threat researchers at IBM Security's X-Force are finding that attackers have even begun coupling disk wipers with encryption to increase success and heighten the urgency of responding to their demands. Not only would victims have to recover the data, they would have to recover the whole operating system, making the recovery that much harder and thus pressuring victims into paying the ransom. All of these issues raise the following questions:

How aware are organizations, especially those representing SMEs and state and local government, of the tools available to combat this threat?

What do organizations need from vendors to better address the threats?

Is the biggest problem they face in addressing the threat a lack of solution awareness, or a lack of resources to acquire, deploy, and manage these safeguards?
Securing Cloud Workloads: How IT Security Pros Grade Their Own Progress
Quarter 2, 2020
PAULA MUSICH

Cloud usage is here to stay, even as computing models in the cloud continue to evolve from virtual machines to containers to new serverless architectures. Security practitioners are still struggling to catch up, even after years of cloud migration. That struggle will only get harder as the momentum behind cloud computing accelerates, and as enterprises embrace a multi-cloud strategy. IT security operations are still labeled as the department of No, and the department of Slow as application developers adopt CI/CD methodologies for cloud applications.

How far have security practitioners come in their effort to bring better security controls to those cloud workloads? Do they understand what they are responsible for and how to implement the appropriate protections? Are they having any success in engaging LOB leaders in working to ensure the security of the workloads leaders are moving to the cloud? As their organizations pursue a multi-cloud strategy, are security practitioners putting a framework in place to secure workloads and data across various cloud architectures? This research project will ask IT security professionals to grade their progress in securing the burgeoning number of cloud workloads across their organizations without imposing a performance tax on end users and developers. Where are they seeing their greatest success? Where are they failing? How are they engaging with LOB leaders and other shadow IT consumers? What do they believe they need from cloud security providers to be successful?

Shifting Security Left: Improving Application Security in the Brave New World of CI/CD
Quarter 3, 2020
PAULA MUSICH

As more organizations adopt the CI/CD methodology, security and development teams must adapt to ensure that applications remain secure without introducing bottlenecks to the release of critical new functionality. What strategies are security practitioners putting in place to adapt to this fast new way of releasing software? What tools are they using? How are they engaging with the development organization to keep pace and ensure that vulnerabilities and even malware aren’t being injected into new applications through open-source code reuse? How are they adapting to DevOps/DevSecOps? This research will survey IT security professionals to better gauge how they are adapting to the move to microservices and open-source software, and what they are doing to ensure the security of those constantly updated applications.
End-User Security Awareness Training: We Gotten Any Smarter About How the Bad Guys Work?

Quarter 4, 2020
PAULA MUSICH

By some estimates, 90% of cyber insurance claims stem from end-user error or bad behavior. Whether it’s malicious or clueless, end users are more often than not the weak link in the chain of defenses that security pros put in place to protect their organization’s critical information assets. EMA explored the use of security awareness training in 2015, but much has changed in the last five years. Since then, the bad guys have gotten even better at social engineering, and breaches still happen as a result of users clicking on malware-laden weblinks or attachments. How has the training evolved over that time? Are more organizations working with end users to improve their threat awareness? How can you measure the success of an end-user training program? This research will look at how security awareness training has evolved in the last five years, what progress IT security pros have made in improving end-user awareness, and what’s not working.

The SecOps Handshake from Both Sides of the Equation

Quarter 4, 2020
DENNIS DROGSETH/PAULA MUSICH

This research will build on EMA’s groundbreaking 2017 study, “SecOps: Integrating Security for Performance, Asset Optimization, and Change Management—Two Views” in providing a clear 2020 roadmap of how security and operations are (or are not) progressing in working together more effectively in a variety of use cases, including the increasingly critical requirements of digital transformation. More specifically, these will include:

- Shifting role relationships, priorities, technology options, and shared metrics between security (cyber detection, risk/compliance, and fraud) and operations, development, and IT service management (ITSM) teams
- Obstacles and benefits along the way
- Impacts of changing requirements given cloud, agile/DevOps, mobile, digital transformation, and other trends
- Technologies that are leading in unifying SecOps initiatives and improving SecOps’ overall effectiveness as viewed from both sides (security and operations)

Learn More

For more information on upcoming EMA research studies, please contact an EMA business development manager at +1.303.543.9500 or sales@enterprisemanagement.com.

About Enterprise Management Associates® (EMA)

Founded in 1996, EMA is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA’s clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.