



# THE STATE OF AUTOMATION IN SECURITY

---

AN ALGOSEC SURVEY  
SPRING 2016

SHARE THIS RESEARCH ON:



## Executive Summary

---

Today's enterprises are continuously evolving to support new applications, business transformation initiatives such as cloud and software defined data centers (SDDC), as well as fend off new and more sophisticated cyber-attacks. With the increasing pace of business, many transformation initiatives are geared towards greater agility and efficiency and the automation of business processes. Security processes however, are still mostly manual, and need to be performed by experienced security engineers who are in increasingly short supply. As a result security has become a bottleneck to business enablement – which not only impacts business agility, but exposes the enterprise to security risks and hampers its ability to address the modern threat landscape.

To understand the prevalence of automation to handle security processes, AlgoSec recently conducted a global survey of 350 C-level executives and senior security and network professionals.

Key takeaways include:

- **Not enough automation.** Only 15% of respondents reported that their security processes were highly automated. Over 52% had some automation in place but felt it was not enough, and 33% said they had little to no automation.
- **Everyone wants more.** Over 83% of respondents stated that the use of automation in security needs to increase over the next 3 years.
- **Motivations for automation abound, but so are concerns.** The growing number of cyber threats, time spent performing security changes manually, and cloud and SDN projects were the top motivations for automation. However, concerns about accuracy, knowledge and resources required to implement as well as difficulty driving organizational changes, are inhibiting the proliferation of automation tools across the organization.
- **Automation serves the business.** Over 80% of respondents believe that automation will increase the overall security posture of their organizations, while 75% think it will improve application availability. 75% also feel that automation will reduce audit preparation time and improve compliance. Half of all respondents - 50% - believe that automation will help deal with the IT skills shortage and reliance on experienced security engineers.

As the survey shows, there is a critical need for automation in security. Currently, highly skilled engineers are spending their valuable time 'keeping the lights on' – manually maintaining existing systems, sifting through countless security alerts, and making device configuration changes – changes which are inadvertently causing outages and security holes. While not a replacement for intelligent human analysis, survey respondents believe that automation can replace much of the 'grunt' work and repetitive tasks, alleviating some of the pressures on IT and helping to free up time to work on critical security and strategic business initiatives.

However if the full benefits of automation are to be realized there first needs to be better communication between those handling the day-to-day IT network and security operations and their senior management. Today, C-level executives do not appear to fully understand the daily challenges faced by their staff and the solutions available to address them. As C-level executives become more educated, automation should be driven from the top down in order to alleviate concerns surrounding accuracy, processes and business disruption.

## The State of Automation in Security

Overall, 15% of survey respondents reported that their security processes were “highly automated” today, while 52% had some automation in place but felt it was not enough, and 33% said they had little or no automation at all.

### C-Level execs misinformed about level of security automation in their organizations

C-Level executives however had a notable difference of opinion. Only 7% claimed that their organizations were “highly automated” and 45% reported that they had little to no automation in place. These findings indicate that there is potentially a disconnect between respondents handling the day-to-day security operations and their senior management. C-Level execs may not fully understand the daily challenges faced by their staff, and the solutions available to address them and ensure the best utilization of resources.

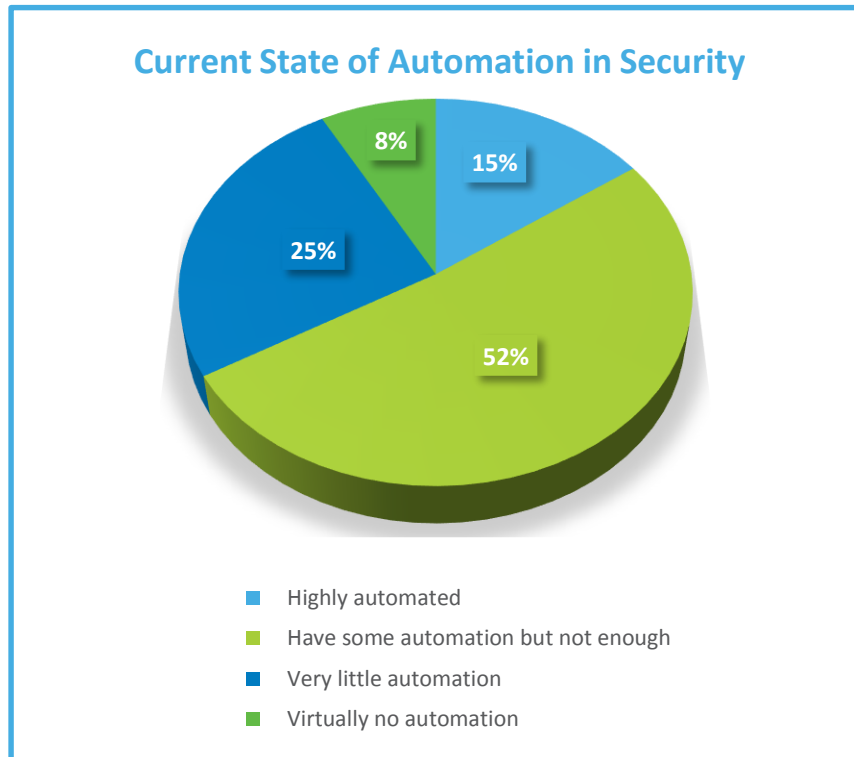
### Medium sized organizations least likely to utilize automation

There were also differences in responses based on the size of the organization. Only 9% of medium sized organizations (1001-5000) were “highly automated” while 15% stated that they had “virtually no automation”—significantly higher than the overall average (8%). This is quite surprising given that the case for automation typically increases with the size of the organization.

On the other hand, the survey showed that smaller organizations are utilizing automation more, most likely to free up their IT team to concentrate on more technically demanding work, while larger enterprises are more likely to rely on automation in order to reduce complexity.

### Finance and energy most automated, telecoms organizations at risk

As expected, given their heavy reliance on networks for day-to-day operations and the direct link between uptime and revenue, organizations in the finance and energy sectors were most likely to utilize

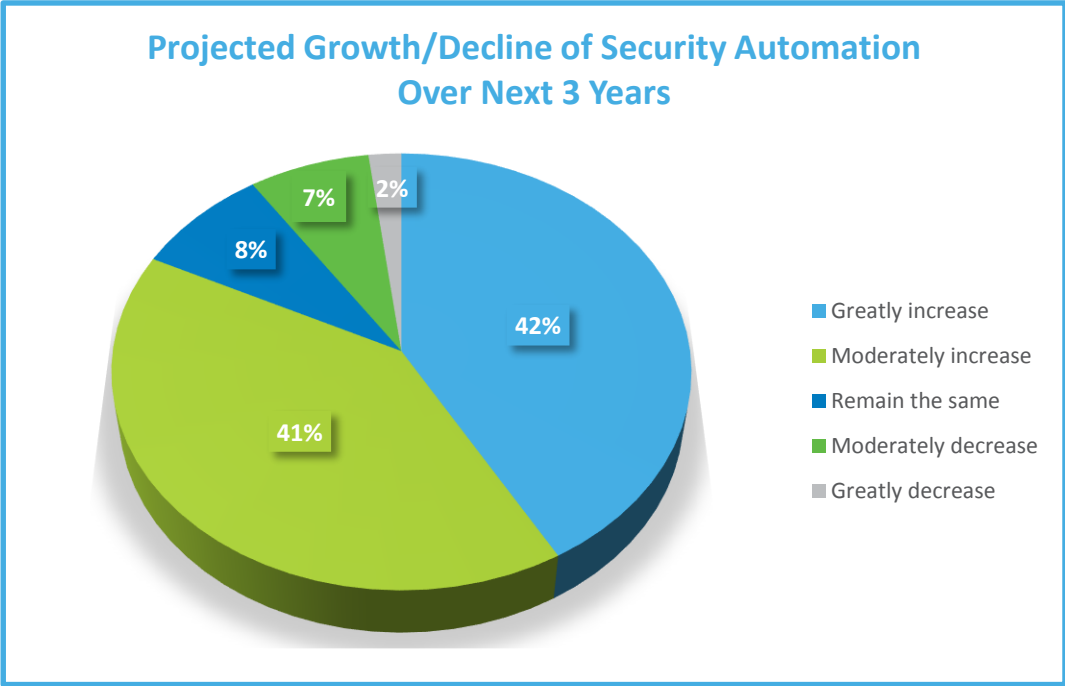


automation in their security processes. 71% of respondents from the finance sector and 77% of respondents in the energy sector said they were either “highly automated” or had “some automation”.

Surprisingly, given the impact on customer relations and revenues caused by downtime, the telecoms sector was among the least likely to be “highly automated” (7%), with 40% reporting they had “little automation” compared to the average 25%. This may be one of the reasons for the relatively high number of network and application related outages experienced by telecom companies and their customers over the past few months.

### The Future of Security Automation - We Want More

Overall, respondents reported that they expect the use of automation to manage security to increase, with 83% saying it should either moderately or greatly increase over the next three years.



## Key Drivers for Automation: Mixed Motivations

---

The top drivers for security automation identified overall were (in order of priority):

- 1 Cyber threats and the number of alerts
  - 2 Too much time spent on manual tasks
  - 3 Hackers using automated tools, so an automated defense is required
  - 4 Cloud and SDN projects
  - 5 Difficulty hiring experienced security staff
- 

Not surprisingly security staff were primarily concerned with utilizing automation to address cyber threats, whereas network operations staff and data center architects both see considerable value in automation for cloud and SDN projects – indicating a desire to support business transformation and agility initiatives.

It's also interesting to note that C-level executives ranked “too much time spent on manual tasks” as the biggest driver and cyber threats as second, reversing the overall rankings. This reveals a difference in priorities for top-level management, with their focus being on how resources can be better utilized, rather than on how automation can enhance an organization's overall security posture.

## Inhibitors to Automation: Is it Accurate? How Do We Do It?

The biggest inhibitors to increasing automation in security operations were identified as the following (in order of priority):

All Roles Excluding CIOs	CIOs
<b>1</b> Concerns about accuracy and false positives	<b>1</b> Lack of tools that provide the necessary automation capabilities
<b>2</b> Difficulty driving organizational changes	<b>2</b> Concerns about business disruption
<b>3</b> Don't have the time to dedicate to implementing automation	<b>3</b> Concerns about accuracy and false positives
<b>4</b> Lack of tools that provide the necessary automation capabilities	<b>4</b> Don't have the time to dedicate to implementing automation
<b>5</b> Lack of knowledge on how to automate processes	<b>5</b> Lack of knowledge on how to automate processes
<b>6</b> Concerns about business disruption	<b>6</b> Difficulty driving organizational changes

Interestingly, C-level executives and network operations staff rated a lack of tools that provide automation capabilities as their top inhibitor, differing from the overall results which put concerns about accuracy and false positives first. Understandably, C-level executives were also concerned about business disruption, whereas respondents in other roles mostly listed it fifth or sixth.

### Fear factor holding organizations back

These results reinforce the conclusion that C-Level executives aren't informed enough about automation tools, while those within an organization who are actually doing the work are too afraid about potential errors to put forward a case for automation. This highlights that automation has to be a top-down initiative, otherwise deployments will be impeded by staff concerned about accuracy and false positives.

## Without Automation: What Is IT Doing All Day?

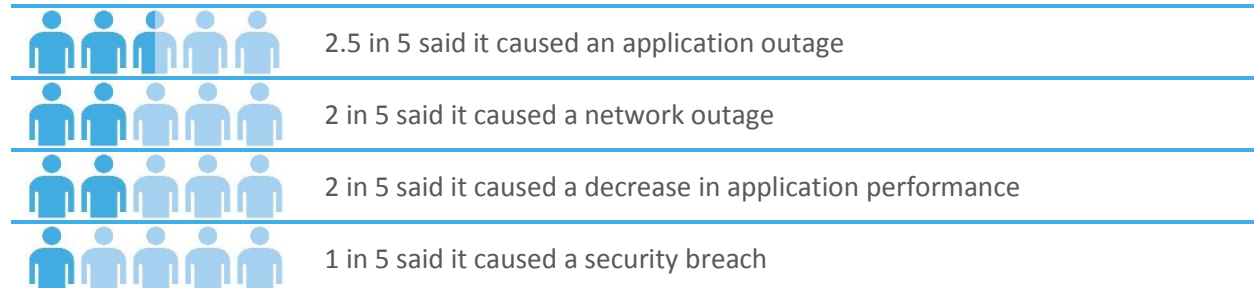
In the absence of automation, when asked where the IT team currently spends most of its time, respondents identified the following areas as being resource intensive (in order of priority):

- 1 Ongoing security configuration and change management
- 2 Incident response and/or remediation
- 3 Large complex deployment projects
- 4 Vulnerability analysis and patching
- 5 Monitoring and intrusion prevention
- 6 Compliance preparation and audits
- 7 Deployments of new security solutions

Again there were some slight variations in responses depending on job role and day-to-day focus. Network operations staff listed incident response and/or remediation first, while data center architects put large complex deployment projects top of the list.

## Manual Processes Cause Outages

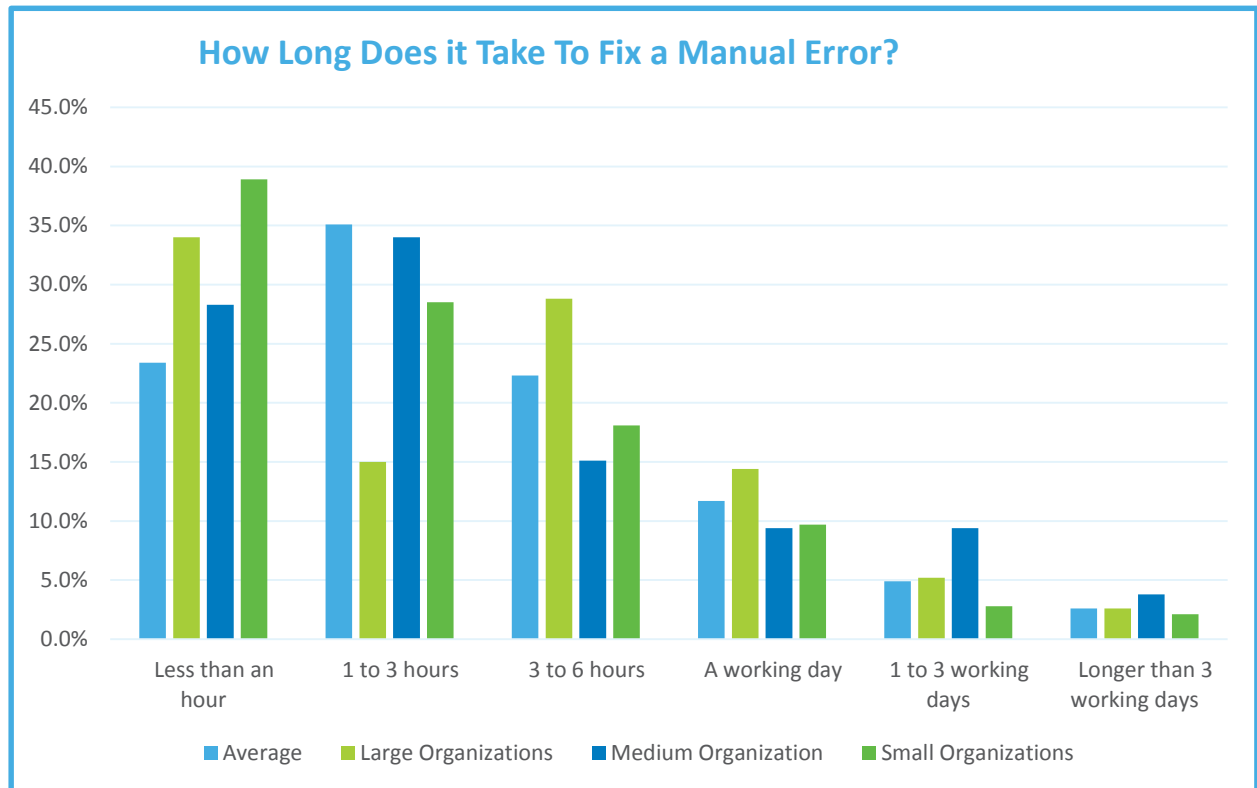
When asked about the impact of manual security change processes in the past 12 months, respondents reported that:



C-level responses differed from the overall average once again. Only 32% of C-level executives reported an application or network outage as a result of manual configuration errors—considerably lower than the average, and only 13% claimed to have experienced a security breach as a result of a manual security change, as opposed to 20% overall.

**For 1 in 5 misconfigurations took longer than a day to fix!**

On average, security related errors and misconfigurations caused by manual processes took 1-3 hours to fix (35% of respondents), with 22% of issues taking 3-6 hours to fix, while 19% of respondents said that problems took a full working day or more to resolve.



Resolution time, however, varied depending on the size of the organization. At large organizations – where the cost of an outage and downtime is typically the highest, as is the complexity of the environment – 29% of respondents said it took 3-6 hours to fix a problem caused by manual security process errors, 22% said that it took a day or more, and only 15% said that it took less than an hour to fix. Similarly, 23% of medium size organizations said that it took over a day to fix a problem.

The average cost of a data center outage in 2016 will be \$740,357<sup>1</sup>








Interestingly 36% of C-level executives believed issues took 3-6 hours to fix compared to the average 22% and only 10% believed a problem took a day or more to fix.

<sup>1</sup> Ponemon Institute, 2016 Cost of Data Center Outages Report



## Yes to Security Process Automation

Respondents identified a wide range of benefits from automating security processes, many of which are tied to business agility and compliance rather than directly to security. Interestingly, the results were pretty uniform across job titles, company size and industry (with nominal deviations).

	3.25 out of 4 believe automation will increase the overall security posture of an organization
	3 out of 4 believe automation will improve application availability by reducing outages
	3 out of 4 believe automation will eliminate mistakes that create access points for hackers
	3 out of 4 believe automation will reduce errors and process security policy changes faster
	3 out of 4 believe automation will reduce audit preparation time and improve compliance
	2 out of 4 believe automation will help deal with the IT skills shortage
	2 out of 4 believe automation will reduce the need for domain and/or vendor technology experts

## Conclusions and Recommendations

---

It is clear that organizations of all sizes and industry sectors are struggling to manage security processes across their ever changing and increasingly complex networks. Changing security configurations, responding to cyber threats and rolling out new, large-scale IT initiatives are severely hindered by tedious, time-consuming, and error prone manual processes. This in turn directly affects the organization's security posture and increases risk, not to mention causes outages and impedes business transformation.

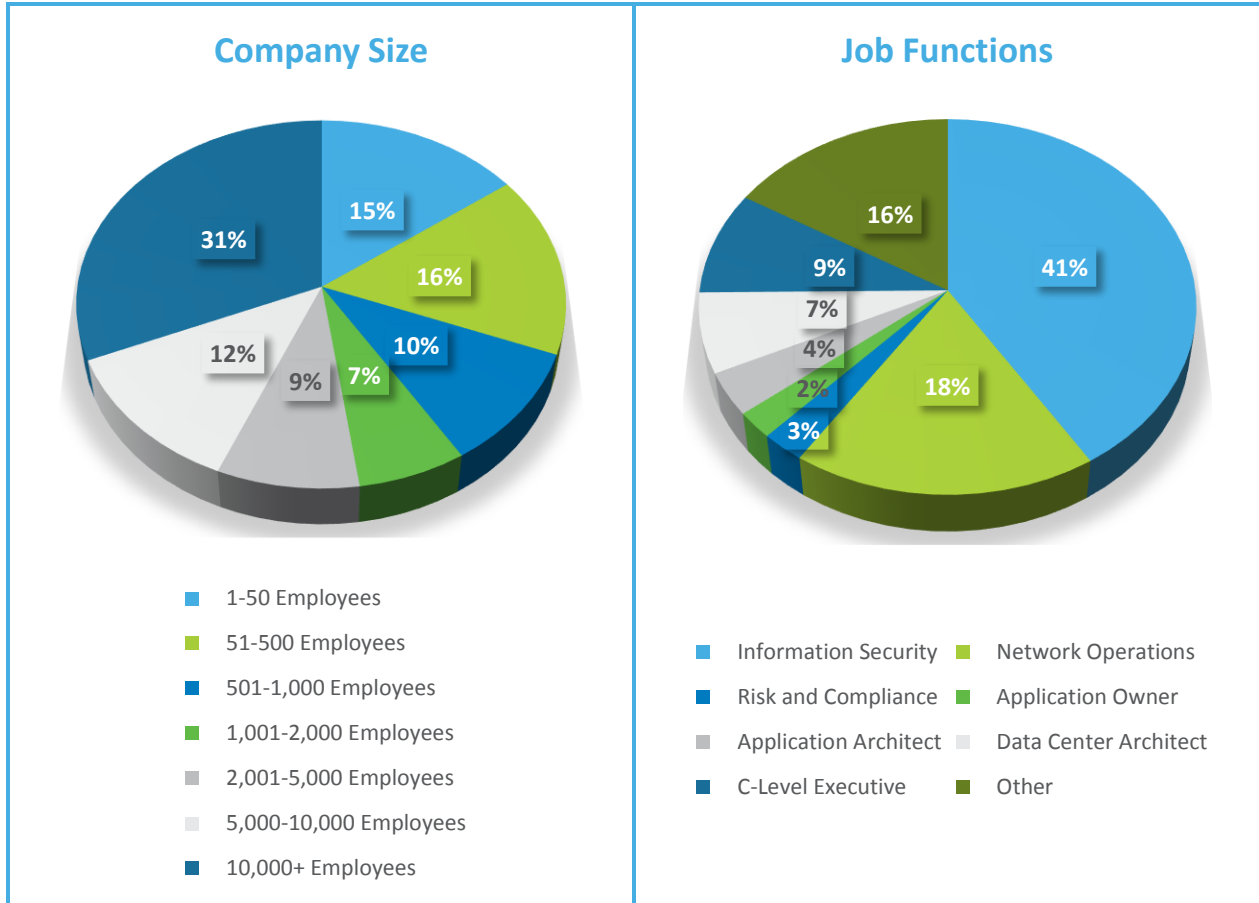
Hand in hand with enhanced security, automation will help these organizations improve business agility and availability, increase management and operational efficiencies, and cut down the time and effort needed to support auditing and compliance requirements. While it won't replace human intelligence, automation can replace many of the manual, repetitive tasks currently performed by highly skilled – and highly paid – staff, freeing them to focus on innovation and high-value projects that will deliver a competitive edge for the business. And, in addition to cutting operational expenses, automation can reduce the reliance on 'long-timers' – the guys who retain critical 'tribal knowledge' about the network in their heads, as well as on domain and vendor specific experts.

Key recommendations for implementing automation for security include:

1. **Communicate and educate.** The good news is that C-Level executives are already convinced of the value of automation, but there's a disconnect between those doing the work and their senior management. So get everyone on the same page about the value, benefits and capabilities as well as the limitations of automation.
2. **Executive initiative.** Automation should be driven from the top down in order to ensure a uniform, structured and realistic approach to its implementation across the organization. C-level endorsement should also help alleviate concerns related to organizational changes, deployment resources, processes and expectations, as well as concerns related to staffing – be it changes in roles and responsibilities or possible cutbacks.
3. **Not just for security.** Security changes don't just affect security; they impact almost every other aspect of IT – from business application availability and outages, to migrations to new platforms such as the cloud, regulatory compliance and many other IT-related business initiatives. Therefore all relevant IT disciplines should be involved in the deployment and use of automation—not only because of the security impact on their initiatives, but also because collaborating with security teams through automation can enhance the overall success of their own projects.

## About the Survey

The State of Automation in Security survey was conducted in early 2016 and surveyed 350 IT professionals worldwide.



Respondents represented a wide variety of industries including agriculture, construction, energy and utilities, financial services, government, healthcare, pharmaceuticals and biotech, manufacturing, retail, technology and transportation.

## About AlgoSec

AlgoSec simplifies, automates and orchestrates security policy management to enable enterprise organizations and service providers to manage security at the speed of business. Over 1,500 of the world's leading organizations, including 20 of the Fortune 50, rely on AlgoSec to optimize their network security policy throughout its lifecycle, to accelerate application delivery while ensuring security and compliance. For the past 5 years, AlgoSec has been profitable with an average annual growth rate of 41%. Moreover, since its inception, AlgoSec has been committed to the success of each and every customer, and provides the industry's only money-back guarantee.

For more information visit <http://www.AlgoSec.com> or visit our [blog](#).



**Global Headquarters**  
65 Challenger Road,  
Suite 320  
Ridgefield Park  
NJ 07660, USA  
+1-888-358-3696

**EMEA Headquarters**  
80 Coleman Street  
London EC2R 5 BJ  
United Kingdom  
Tel: +44 207-099-7545

**APAC Headquarters**  
10 Anson Road, #14-06  
International Plaza  
Singapore 079903  
+65-3158-2120

**AlgoSec.com**



© Copyright 2016, AlgoSec Inc. All rights reserved. WP-AUTM-EN-1