BDR Cadence
Competitive Flip Campaign /
Greenfield Campaign w/Automation Focus

Contents

AUTOMATION HIGH-LEVEL STORY

Meet Karen, Chief Information Security Officer. Karen leads security at a FORTUNE 500 company that is rapidly transforming into a hybrid enterprise with a cloud-first focus. This change is helping Karen deliver business agility but is also creating major challenges. Karen's security team is battling with limited visibility across their on-premises, virtual and cloud resources. The team also faces a growing number of security gaps they can't even see, much less manage.

Karen would like to hire more staff, but there's a huge lack of available talent. This leaves her team drowning in manual tasks and moving in so many directions that misconfigurations and other network security mistakes are skyrocketing. At this point, human error is by far the leading cause of cyber security failures in Karen's org—the same problem CISOs and other security leads are facing globally.

Here's what FireMon security automation solutions can do for Karen and her organization.

Karen can gain control of security across her entire hybrid enterprise without having to hire a new fleet of security pros. FireMon eliminates the visibility gaps that plague hybrid networks, and enables her team to respond automatically, and rapidly, to attacks.

FireMon automation frees Karen's overburdened staff from mundane but necessary manual tasks, streamlines change management workflows, and more. In short, FireMon automation helps Karen's team eliminate a huge source of human error, bolster security, and improve their efficiency all at the same time—driving down costs and freeing staff for higher-value tasks.

AUTOMATION ELEVATOR PITCH

FireMon helps businesses use security automation to solve some of their toughest challenges. One of them is using automation to eliminate misconfigurations caused by human error, which can cause unplanned outages, compliance issues, and leave gaps for breaches. Another is getting visibility throughout multi-cloud or hybrid cloud environments. Wherever a business is on the path to security automation, we can help.

AUTOMATION TALKING POINTS

1. **"I can't find any security pros!"**

   There is an intense and growing lack of cybersecurity professionals.

   - CSO Magazine. July 29, 2019. "Only half of businesses believe they're capable of developing and retaining cybersecurity expertise."

   - ISSA. May 9, 2019. "In the third annual global study of cyber security professionals by the Information Systems Security Association (ISSA) and independent industry analyst firm Enterprise Strategy Group (ESG) found that the cyber security skills shortage impacts **74% (almost 3/4ths)** of organizations."

2. **"Automate or Die!!!👌💯😜"**

   Embracing security automation is a key strategy for most enterprises.

   - Dark Reading. Apr 18, 2019. "A survey of by the Ponemon Institute found that that most organizations today are placing bets on security automation. Approximately 79% of respondents either use automation currently or plan to do so in the near-term future."

3. **"Without automation, we are TOAST!"**

   Automation is the only viable solution to maintaining consistent security in the cloud era.

   - InfoSecurity Magazine. Aug 6, 2019. "It is essential to invest in automation, because **otherwise, it is impossible** to ensure consistent security policies are deployed."

   - SCMagazine. July 23, 2019. "The scalability cloud platforms provide is one of the key benefits that organizations are looking to take advantage of, but it's that same scalability that can make security measures incredibly difficult to implement and manage. Automated cloud security is essential to mitigate risk in these environments."

4. **"Do you even automate, bro?"**

   Automation is becoming the new normal because of the cybersecurity skills gap.

   - TechTarget. Aug 12, 2019. "What used to be considered forward-thinking of CISOs who implemented cybersecurity automation is now the standard."

   - Security Boulevard. Aug 9, 2019. "Automation can help deliver greater efficiencies for processes, and that could ease the burden caused by the cyber security skills gap."

5. **"We're breaking our own security!"**

   Automation enables faster response time and reduces human error.

   - Gartner. Feb 21, 2019. "Gartner predicts that through 2023, 99% of cloud security failures will be the result of human error."
   - Enterprise Security Magazine. Aug 6, 2019. "With automation, systems can respond to attacks with minimal time lag and without human intervention. Automation helps eliminate human error to minimize the occurrence of false positives."

AUTOMATION USE CASE SNIPPETS

1. Threat and Vulnerability Management

MICRO FORM

A customer needed help integrating SOAR-triggered changes and blocking malicious IP addresses across multiple firewall vendors. FireMon enabled them to make real-time policy changes across all their vendor solutions in just minutes.

SHORT FORM

A customer approached FireMon for help integrating SOAR-triggered changes and blocking malicious IP addresses across multiple firewall vendors. FireMon enabled them to make policy changes in real-time across their entire roster of vendor solutions, reducing the time frame to globally block malicious actors from once a day to just a few minutes.

LONG FORM

Mitigate threats in an instant with integrated security management

A customer approached FireMon for help integrating SOAR-triggered changes across multiple firewall vendors and blocking malicious IP addresses across all vendors. FireMon enabled the client to make policy changes in real-time across their entire roster of vendor solutions, reducing the time frame to globally block malicious actors from once a day down to just a few minutes and ensuring that their networks are always protected. FireMon's policy automation solution speeds response times and allows security teams to unleash the full potential of SOAR to:

- Speed up policy management changes by 5x
- Automate and optimize workflows to reduce manual errors
- Make policy changes in real-time, ensuring that your networks are always protected
- Orchestrate a variety of security tools to optimize your organization's security posture

2. Hybrid Cloud

MICRO FORM

A customer needed help achieving full visibility and unified security policy management across their hybrid environment. FireMon enabled them to discover, map and analyze all enterprise connectivity, both on-premises and in the cloud.

SHORT FORM

A customer approached FireMon for help achieving full visibility and unified security policy management across their hybrid environment. The FireMon platform enabled them to discover, map and analyze all enterprise connectivity, both on-premise and in the cloud, delivering continuous identification of and protection for new devices, routers, and cloud connectivity.

LONG FORM

Quickly and easily update complex, hybrid environments

A customer approached FireMon for help achieving full visibility and unified security policy management across their hybrid environment. While investments in new cloud technology were made, the tools and processes for firewall configurations were at least a decade old. The FireMon platform enabled them to discover, map and analyze all enterprise connectivity, both on-premise and in the cloud, delivering continuous identification of and protection for new devices, routers, and cloud connectivity, allowing the customer to reduce their attack surfaces. FireMon makes it possible to:

- Accelerate application migrations to the public cloud
- Minimize business disruptions
- Avoid application outages during and after the migration

3. SLAs

MICRO FORM

FireMon provides intelligent risk scoring, automated compliance checks, automated ticket tracking and automatic rule base analysis to prevent unnecessary or rule-violating changes. This provides efficiency to free teams up for other tasks.

SHORT FORM

FireMon provides intelligent risk scoring, automated compliance checks, automated ticket tracking and automatic rule base analysis to prevent unnecessary changes. FireMon enables automated approvals for low-risk changes and can automatically create tickets for rule removal. FireMon clients report benefits including enhanced visibility and the ability to fast track or deny requests, giving them efficiency to free teams up for other tasks.

LONG FORM

Eliminate pressure by automation review and change processes

FireMon provides intelligent risk scoring along with automated compliance checks to let you know if the change meets rule requirements or should be rejected. FireMon automates ticket tracking, storing detailed ticket requests that capture all relevant and required information upfront. FireMon automatically analyzes your rule base for similar or already existing access to prevent unnecessary changes and provides insight into any requests that duplicate access that is already accounted for, as well as any rules that allow similar access to a new request. FireMon enables automated approvals for changes which you identify as low-risk and can automatically create tickets for rule removal. FireMon clients report benefits including application guard rails, enhanced visibility, and the ability to fast track or deny requests, therefore giving them the efficiency they need to free teams up for other tasks.

FireMon Automation enables customers to:

- Reduce the number of compliance violations by checking compliance proactively prior to implementation
- Prevent human errors that increase the enterprise attack surface
- Remove the friction between DevOps and SecOps to deliver security at speed and improve SLAs
- Integrate seamlessly with their unique infrastructure through a robust, RESTful API to simplify automation, and ease migration to next-gen networks

4. Application Abstraction

MICRO FORM

A customer needed help reducing the time their security team was spending on manual tasks. FireMon provided intent-based security and orchestration through application abstraction, delivering time savings and increased efficiency.

SHORT FORM

A customer approached FireMon for help reducing the time their security team was spending on manual tasks. FireMon gave them the ability to correlate policies with services and applications, set abstracted definitions of the required access, and then automatically translate that into the proper configuration of security policy on the enforcement points. The customer reports time savings and more efficiency.

LONG FORM

Eliminate tedious manual work to focus on mission-critical tasks

A customer approached FireMon for help in reducing the excessive amount of time their security team was spending on manual tasks. FireMon gave them the ability to determine which policies correlate to which services and applications, and then, using known-good baseline configurations for each application, set up an abstracted definition of the required access, and then automatically translates that into the proper configuration of security policy on the enforcement points. Our customer now enjoys time savings and more efficiency as their teams can fast track requests and changes and they are able to focus on more strategic and innovative tasks.

With FireMon's Automation, you can expect:

- Continuous, intent-based security, and orchestration;
- Sub-second delivery of compliant security configurations through automation
- Clear visibility into application connectivity; and the agility to accelerate speed to market

5. CPOC

MICRO FORM

A customer needed to reduce the time their firewall admins spent writing manual rules. FireMon Automation gathered policies from firewalls and other security platforms and tools under one central point of control, dramatically improving efficiency.

SHORT FORM

A customer approached FireMon for help with central firewall policy management because their firewall administrators were spending 35% of their time writing manual rules, which resulted in occasional manual errors. FireMon Automation enabled the customer to bring together policies from firewalls and other security platforms and tools under one central point of control, with the ability to implement policy across applications and devices as needed.

LONG FORM

Eliminate manual, redundant workloads with a central point of control

A customer approached FireMon for help addressing network visibility, efficient and timely clean up, and central firewall policy management because their firewall administrators were spending 35% of their time writing manual rules for 25 firewalls. With only three administrators to manage the work, there were also occasional manual errors, setting the customer up for a potential breach, or costly downtime that could lead to revenue loss. FireMon Automation enabled the customer to bring together policies from other security platforms, firewalls, vulnerability scanners, and other tools under one central point of control. The customer is now reaping the benefits of extracting management from several firewall devices into one central console with the ability to implement policy across applications and devices as needed.

FireMon Automation enables customers to:

- Reduce the number of compliance violations by checking compliance proactively prior to implementation
- Prevent human errors that increase the enterprise attack surface
- Remove the friction between DevOps and SecOps to deliver security at speed and improve SLAs
- Integrate seamlessly with their unique infrastructure through a robust, RESTful API to simplify automation, and ease migration to next-gen networks

6 WEEK CADENCE TIMELINE

Gifts – Sendoso template

Gifts – Followup Email

Day 1 – Email, personalized with room for a block of text to be added on a specific use case and a note that BDR will be reaching out via LinkedIn as way of introduction

Day 1 – LinkedIn message + connection request + ROI calculator link

Day 2 – Phone call (mention ROI calculator)

Day 5 – Email asking if they are interested in taking the Forrester Automation Maturity Assessment

Day 5 – LinkedIn view

Day 8 – LinkedIn message with link to Forrester Automation Maturity Assessment

Day 8 – Phone call (mention Forrester Automation Maturity Assessment and Report)

Day 10 – LinkedIn view

Day 10 – Phone call

Day 11 – LinkedIn message with link to FireMon Automation: Private & Hybrid Clouds infographic

Day 14 – Email with stats from Dark Reading Sponsored Report and ask if they'd like to see it

Day 14 – Phone call

Day 17 – Email with coffee e-gift card to all contacts in the cadence with link to Top 10 Security Misconfigurations

Day 18 – LinkedIn View

Day 21 – Email referencing the FireMon Automation: Integrated Threat & Vulnerability Mgmt infographic and asking if they'd like it

Day 21 – Phone call (mention the coffee e-gift card)

Day 25 – LinkedIn message with link to FireMon Automation: Central Point of Control infographic

Day 25 – Phone call

GIFTS

Sent to two contacts at the account.

Recommend mid-level (Security Director or Project Manager responsible for Security project).

- Include a personalized note. Sample below. Number of characters will depend on the type of gift sent**. Cookies are performing the best.**

1. Sendoso Gift message

Template: Customize this for a particular target	**Example:** Tile, Tim Drake, Wayne Industries
[NAME], IT Security is tough. So we make some sweet automation solutions. Enjoy the [GIFT]! I'll be in touch. [BDR NAME] [BDR PHONE] [BDR EMAIL]	[NAME], IT Security is tough. So we make some sweet automation solutions. Enjoy the cookies! I'll be in touch. Jason Todd 111-111-1111 Jason.Todd@firemon.com

2. Cookie Follow-up Email

Subject: Did you get the cookies?

Template	**Template**
Hi [NAME], I hope you enjoyed the cookies I sent earlier this week. I wanted to see if we could find a time to chat about security automation at [COMPANY]. Many of our customers tell us security automation is a top priority – where does it fall for you and your team? I look forward to speaking with you. Best,	Hi Tim, I hope you enjoyed the cookies I sent earlier this week. I wanted to see if we could find a time to chat about security automation at Wayne Industries. Many of our customers tell us security automation is a top priority – where does it fall for you and your team? I look forward to speaking with you. Best,

DAY 1

1. Email

Subject: Re: Did you get the cookies?
or
COMPANY NAME + FireMon Automation

Template	Example
[NAME], [CUSTOMIZED INTRO] If so, you're not alone. For example, [SNIPPET]. [NAME], would you have time for a quick chat on how automation can help you do more with less at [COMPANY]? I'll reach out to connect soon on LinkedIn. Best,	Tim, From your LinkedIn profile it appears you are heavily involved with firewall change management at Wayne Industries. In your role as Security Director, are your finding it challenging for your team to keep pace with your organization's needs? If so, you're not alone. For example, a FireMon customer needed to reduce the time their firewall admins spent writing manual rules. Our Automation solution gathered policies from firewalls and other security platforms and tools under one central point of control, dramatically improving efficiency. Tim, would you have time for a quick chat on how automation can help you do more with less at Wayne Industries? I'll reach out to connect soon on LinkedIn. Best,

2. LinkedIn

Template	Template
[NAME], What kind of return would you expect on an investment in security automation? I recently sent you an email on the topic, and I wanted to connect with you here on LinkedIn. In particular, I wanted to share this link to our ROI Calculator—it provides useful ballpark figures to serve as a starting point. Would you have time for a quick call? Best, [SEND CONNECTION REQUEST]	Tim, What kind of return would you expect on an investment in security automation? I recently sent you an email on the topic, and I wanted to connect with you here on LinkedIn. In particular, I wanted to share this link to our ROI Calculator—it provides useful ballpark figures to serve as a starting point. Would you have time for a quick call? Best,

DAY 2

Phone

- Mention that you are following up on an email and LinkedIn message
- Mention ROI calculator

DAY 5

1. Email

Subject: Re: Did you get the cookies?
or
Re: COMPANY NAME + FireMon Automation

Template	**Example**
[NAME],	Tim,
The analyst firm Forrester has created an assessment tool to help you determine the maturity level of your automation infrastructure, and to identify competencies you need to strengthen or development at [COMPANY].	The analyst firm Forrester has created an assessment tool to help you determine the maturity level of your automation infrastructure, and to identify competencies you need to strengthen or development at Wayne Industries.
Would you be interested in taking the assessment? I'd be happy to send along a link.	Would you be interested in taking the assessment? I'd be happy to send along a link.
Just let me know—I look forward to hearing from you.	Just let me know—I look forward to hearing from you.
Best,	Best,

2. LinkedIn View

Simply log into LinkedIn and VIEW the prospects' profile, without sending a message. Your photo and name will pop up in their feed.

DAY 8

1. LinkedIn

Template	Example
[NAME],	Tim,
Are you automating infrastructure to remain competitive in the [INDUSTRY] sector?	Are you automating infrastructure to remain competitive in the Technology sector?
Embracing automation effectively will set leaders apart from laggards. Find out where you stand with Forrester's Automation Maturity assessment tool.	Embracing automation effectively will set leaders apart from laggards. Find out where you stand with Forrester's Automation Maturity assessment tool.
Once you complete the assessment, I'd be happy to review the results with you and plan out next steps.	Once you complete the assessment, I'd be happy to review the results with you and plan out next steps.
Best,	Best,

2. Phone

- Mention that you are following up on a LinkedIn message
- Mention the link to the Forrester Automation Maturity assessment tool. The full name of the document is "***Gauge Your Infrastructure Automation Maturity Assessment***: *The Infrastructure Transformation Playbook*"

DAY 10

1. Phone

- Mention that you are following up on a LinkedIn message
- Mention the link to the Forrester Automation Maturity assessment tool. The full name of the document is "**Gauge Your *Infrastructure Automation Maturity Assessment***: *The Infrastructure Transformation Playbook*"

2. LinkedIn View

Simply log into LinkedIn and VIEW the prospects' profile, without sending a message. Your photo and name will pop up in their feed.

DAY 11

LinkedIn

Template	**Example**
[NAME],	Tim,
Are complex hybrid cloud environments causing stress for your security teams?	Are complex hybrid cloud environments causing stress for your security teams?
Eight out of 10 organizations are challenged with the complexity of security tools for hybrid cloud environments.	Eight out of 10 organizations are challenged with the complexity of security tools for hybrid cloud environments.
But FireMon offers a better way to control and gain visibility into networks and process changes.	But FireMon offers a better way to control and gain visibility into networks and process changes.
May I send you this infographic?: *Today's Hybrid Environment: Is Your Security Up To Date?*	May I send you this infographic?: *Today's Hybrid Environment: Is Your Security Up To Date?*
Hope to hear from you soon!	Hope to hear from you soon!
Best,	Best,

DAY 14

1. Email

Subject: Re: Did you get the cookies?
or
Re: COMPANY NAME + FireMon Automation

Template	**Example**
[NAME],	Tim,
Curious what's top of mind for other security practitioners?	Curious what's top of mind for other security practitioners?
Dark Reading conducted a surveyed to find out. They gained insights into: • What they are worried about and what makes them feel confident What's working and what isn't • What they see as their teams' greatest challenges • What they would change if they could	Dark Reading conducted a surveyed to find out. They gained insights into: • What they are worried about and what makes them feel confident What's working and what isn't • What they see as their teams' greatest challenges • What they would change if they could
Want to see how [COMPANY NAME's] security team's experience stacks up? I'd be happy to send you the report.	Want to see how Wayne Industries' security team's experience stacks up? I'd be happy to send you the report.
Best,	Best,

2. Phone

- Mention that you are following up on an email; consider dropping stats from the report, such as:
    - Firewalls were among the top three ways cited to protect enterprise data, along with encryption and multifactor authentication
    - Only 3 in 10 respondents found DevOps / SecDevOps to be effective
    - Almost 60% of cybersecurity teams say they do not spend enough time on preventing intrusions
- Mention the Dark Reading Sponsored Report and offer to send it

DAY 17

Email

Subject: No subject line needed – automatically populated from Sendoso (Says: SENDER NAME is sending you a Cup of Coffee!)

Template	**Example**
[NAME],	Tim,
I'm sending you an e-gift card for coffee (see below), but first: What would you say is the single greatest cause of security breaches?	I'm sending you an e-gift card for coffee (see below), but first: What would you say is the single greatest cause of security breaches?
If you guessed mistakes your own team makes, you'd be right. We can even tell you which mistakes are most common.	If you guessed mistakes your own team makes, you'd be right. We can even tell you which mistakes are most common.
So here it is! Enjoy a refreshing beverage and dive into the Top 10 Security Misconfigurations.	So here it is! Enjoy a refreshing beverage and dive into the Top 10 Security Misconfigurations.
Best,	Best,

DAY 18

LinkedIn View

Simply log into LinkedIn and VIEW the prospects' profile, without sending a message. Your photo and name will pop up in their feed.

DAY 21

1. Email

Subject: Re: Did you get the cookies?
or
Re: COMPANY NAME + FireMon Automation

Template	**Example**
[NAME],	Tim,
How fast can you shut down vulnerabilities in your network?	How fast can you shut down vulnerabilities in your network?
The minute you discover a malicious IP, the clock is ticking. With FireMon Automation, you can block threats immediately, even across multiple firewalls from your entire set of vendors.	The minute you discover a malicious IP, the clock is ticking. With FireMon Automation, you can block threats immediately, even across multiple firewalls from your entire set of vendors.
I'd like to send you an infographic with some eye-opening facts and figures—do I have your permission to send it?	I'd like to send you an infographic with some eye-opening facts and figures—do I have your permission to send it?
Best,	Best,

2. Phone

- Mention that you are following up the coffee e-gift card
- Mention the Threat Mitigation infographic, and consider throwing in some figures such as:
    - **$3.92 million** – the cost of a data breach in 2019
    - **3.5 million** – the number of forecasted unfilled security roles in 2021
    - **34%** – the percentage organizations who have less than 50% percent of real-time visibility into network security risks and compliance (*Source: FireMon – no link yet)

DAY 25

1. LinkedIn

Template	Example
[NAME],	Tim,
Are you worried that there are things in your network you don't know about?	Are you worried that there are things in your network you don't know about?
Infrastructure now spans the data center, public and private cloud networks, with multiple tools and vendors	Infrastructure now spans the data center, public and private cloud networks, with multiple tools and vendors
But FireMon bring together all policies from other security platforms, from firewalls to vulnerability scanners, into one central point of control.	But FireMon bring together all policies from other security platforms, from firewalls to vulnerability scanners, into one central point of control.
I'd like to share an infographic with some eye-opening facts and figures—do I have your permission to shoot it over to you?	I'd like to share an infographic with some eye-opening facts and figures—do I have your permission to shoot it over to you?
Best,	Best,

2. Phone

- Mention that you are following up on a LinkedIn message
- Mention the FireMon Automation: Central Point of Control, and consider throwing in some figures such as:
    - **78%** of organizations use two or more vendors for enforcement points on their network
    - **34%** of organizations have less than 50% percent of real-time visibility into network security risks and compliance
    - **24%** of organizations aren't sure or wouldn't admit if they failed a compliance audit