Automate & Prevent: Extending the Detect and Respond Paradigm for Proactive, Scalable Security

Solution Brief

SOLUTION HIGHLIGHTS

Detect and Respond (D&R) security is a traditional approach to security. Extending it with Automate and Prevent (A&P) can make an organization's security more efficient, proactive, and scalable.

The combined approach provides:

- Preventing threats before they occur reduces the attack surface and the time and effort required to analyze false positives and false negatives.
- Reduced risk due to fewer successful attacks
- Greater efficiency with automation of repetitive security tasks
- Increased scalability through the automation of workflows

CHALLENGE

Detect and Respond (D&R) is a cybersecurity strategy focused on identifying and mitigating threats after they have entered an environment. This involves continuously monitoring networks, systems, and digital assets to identify and respond to potential security breaches and cyberattacks.

This approach is reactive by nature—it assumes breaches will occur and focuses on identifying and eliminating them as quickly as possible. This type of security remains essential, especially for the identification and containment of novel threats, but can be made much more effective when augmented by proactive strategies like Automate and Prevent as part of the adoption of a Zero Trust Architecture (ZTA).

Figure 1: Envisioning Detect and Respond Supported by Automate and Prevent

APPROACH

Extending the Detect and Respond paradigm with Automate and Prevent enhances the maturity, scalability, and proactiveness of cybersecurity operations.

Traditional Paradigm: Detect and Respond

- Detect: Identify threats, anomalies, or malicious activities using monitoring tools such as SIEM, IDS/IPS, etc.
- Respond: Take actions to contain, remediate, or investigate the incident.

Limitations of this approach include:

- Reactive in nature
- Manual triage is slow
- Resource-intensive and difficult to scale

Extended Paradigm: Automate and Prevent

- Automate the application of security policies, especially for known threats, to prevent incidents from occurring in the first place.
- Benefits include:
  - Reduced incident volume
  - Allow resources to be focused on fewer, novel threats
  - Reduced human error
  - Scalable security operations
  - Increased overall resilience

Evolved Security Paradigm: Detect & Respond Enhanced by Automate & Prevent

The integration of Automate & Prevent with Detect & Respond leads to a more mature, intelligent, and scalable cybersecurity model. This evolved paradigm shifts security left—emphasizing preemptive defense and automation—while maintaining the strength of rapid detection and response.

Phase	Focus	Tools/Technology Used
Automate	Streamline security policies	Automated policy evaluation and enforcement
Prevent	Harden and preempt	IAM, Zero Trust, security baselines, preventive SoD, data-centric controls
Detect	Identify threats	SIEM, EDR, NDR, UEBA, anomaly detection
Respond	Mitigate and learn	IR teams, forensics, reporting, root cause fixes, continuous improvement

Figure 2: The four security phases — their goals and the technologies that drive them.

This model provides a layered, continuous defense lifecycle—proactively reducing risk, rapidly identifying threats, and streamlining containment and recovery. By organizing around these four phases, security teams can maximize coverage, reduce time to resolution, and build long-term resilience into their security operations.

A CLOSER LOOK AT AUTOMATE AND PREVENT

Prevention focuses on keeping attackers out before they can gain a foothold. Key strategies include:

- **Security controls:** Segregation/filtering, encryption/obfuscation, policy-based access.
- **Vulnerability management:** Patching known software flaws.
- **Least privilege:** Restricting user access to only what is needed.

Automation makes your security faster, smarter, and more scalable. In cybersecurity, automation involves using scripts, tools, or platforms to:

- Auto-respond to known threats (e.g., blocking suspicious access or masking sensitive data)
- Auto-patch vulnerable software as updates become available
- Enforce policy automatically (e.g., restrict access or require MFA when risky behavior is detected)
- Automatically flagging anomalies to reduce alert fatigue and focus analyst attention

Examples in action:

- Automatically apply DRM policies to data and files before they are shared
- Block users from exporting and downloading customer records
- Apply filtering and obfuscation policies to prevent unauthorized access to sensitive data in ERP applications
- If a user logs in from an unusual country, auto-enable MFA or block access entirely.

HOW AUTOMATE AND PREVENT STRENGTHENS DETECT AND RESPOND

A combination of Automate and Prevent with Detect and Respond can:

1. **Reduce risk:** Stopping attacks before they occur means less to detect and respond to.
2. **Save time:** Automating repetitive tasks allows security teams to focus on high-priority threats.
3. **Improve Scalability:** Automated workflows can be scaled efficiently.
4. **Ensure consistency:** Automation enforces standardized policy enforcement and reduces the likelihood of human error.

Combining Detect and Respond with Automate and Prevent creates a more robust framework for securing business-critical data. These approaches can be layered to protect the enterprise, before, during, and after an attack.

Function	Role
Prevent	Stop threats from getting in
Automate	Make processes faster & more reliable
Detect	Spot the threats that sneak in
Respond	Act fast to contain & fix them

Figure 3: How Prevent, Automate, Detect, and Respond work together to stop, spot, and resolve threats

Real-World Example:

To fully understand the benefits of combining Detect and Respond with Automate and Prevent, it helps to look at a real-world example.

1. **Automate:** The organization's email system automatically applies security policies to incoming email.
2. **Prevent:** Email filters block most phishing attempts and users are trained not to click on suspicious links.
3. **Detect:** If one gets through and a user clicks, endpoint detection tools identify unusual behavior.
4. **Respond:** A security analyst investigates the incident, resets passwords, and updates the response playbook.

NEXTLABS SOLUTION

Here's how NextLabs implements Automate and Prevent on top of a Detect and Response approach using its Zero Trust Data-Centric Security framework.

Prevent: Proactive Data Protection

NextLabs emphasizes proactive data protection by enforcing least privilege access and need-to-know policies. This is achieved through:

- **Dynamic Data Masking and Segregation:** Sensitive data is obfuscated or separated based on user attributes, ensuring that only authorized personnel can view or access critical information.
- **Real-Time Data Protection:** Using tools like the Data Access Enforcer (DAE), NextLabs secures data at rest and in use by applying encryption and access controls to prevent unauthorized access.
- **Compliance Automation:** The platform automates compliance with regulations such as ITAR, EAR, and EH&S, ensuring data access aligns with legal and regulatory requirements.
- **Enterprise Ditigal Rights Management (E-DRM):** Persistently protects files wherever they go by applying attribute-based policies that control who can view, edit, copy, or share sensitive content.
- **Prevent Data Leakage:** NextLabs prevents unauthorized extraction of data from business-critical applications like SAP, AI systems, and Business Analytics tools by enforcing policies directly at the application layer. These policies leverage application metadata, data classifications, and user context to block unauthorized downloads, data extraction, and distribution. This ensures sensitive business information remains secure and protected from leakage—without disrupting legitimate access or workflows.

Automate: Streamlined Security Operations

NextLabs enhances operational efficiency by automating security processes:

- **Compliance Procedures:** Prompt users to classify attachments and documents before they are shared
- **Policy Enforcement:** Automate masking of confidential data, and filtering of data to enforce logical data segregation.
- **Role Provisioning:** Roles and permissions are assigned automatically based on predefined policies, reducing manual intervention and human error and preventing possible unauthorized access.
- **Audit and Monitoring:** Automated log and evidence collection and report production streamlines the audit and compliance reporting processes

Figure 4: From reactive to proactive: How Automate & Prevent strengthens Detect & Respond

REAL-WORLD IMPLEMENTATION: BOEING

Boeing adopted NextLabs' Zero Trust Data-Centric Security suite to secure its SAP S/4HANA environment and other critical enterprise applications. The implementation included:

- **Attribute-Based Access Control (ABAC):** Policies were defined based on user attributes, ensuring access was granted according to the principle of least privilege.
- **Data Protection Across Global Operations:** The solution delivered consistent data security across Boeing's operations in the U.S. and more than 65 international sites, supporting compliance with global regulations.
- **Enhanced Security Posture:** By consolidating ERP systems and embedding security controls, Boeing improved operational efficiency while safeguarding sensitive data.

By integrating Automate and Prevent strategies, NextLabs enables organizations to enhance their Detect and Respond framework, proactively securing data, streamlining operations, and ensuring regulatory compliance. To learn more about Boeing's implementation, watch Boeing's webinar where they share how they deployed NextLabs Zero Trust Data Security--enabling them to strengthen their security posture and consolidate ERP systems into a unified global instance.

For more details, please see SAPinsider's report, How Boeing Adopts Zero Trust Data-Centric Security with NextLabs.

To learn more about how an Automate and Prevent approach can benefit your organization, explore NextLabs' Intelligent Enterprise page.

NEXTLABS® | Zero Trust Data-Centric Security

ABOUT NEXTLABS

NextLabs®, Inc. provides zero trust data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based zero trust policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, AWS, Accenture, Deloitte, Infosys, and IBM. For more information on NextLabs, please visit: **http://www.nextlabs.com**.