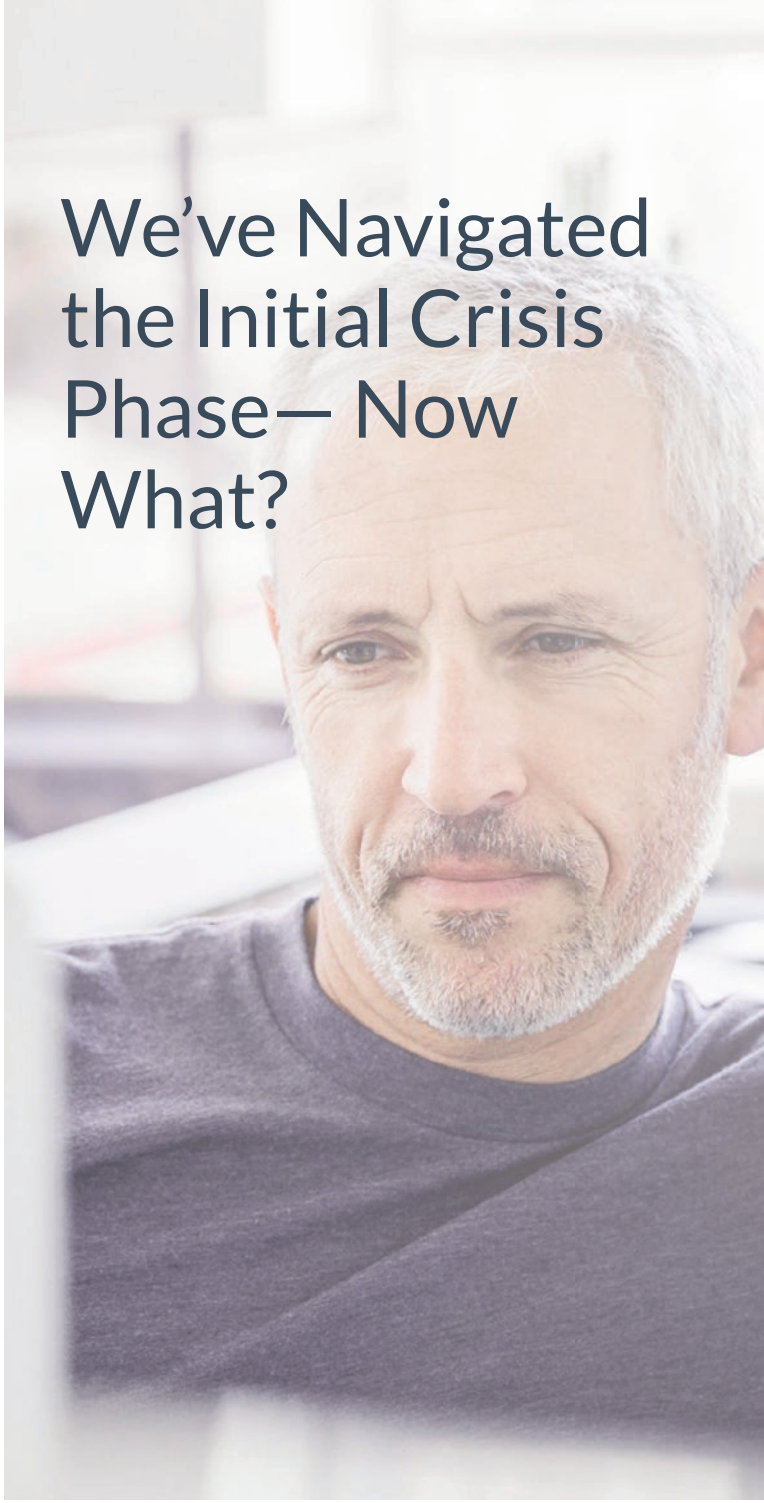
NETWITNESS

5 Ways Security Operations Must Evolve for the Next Normal

We've Navigated the Initial Crisis Phase— Now What?



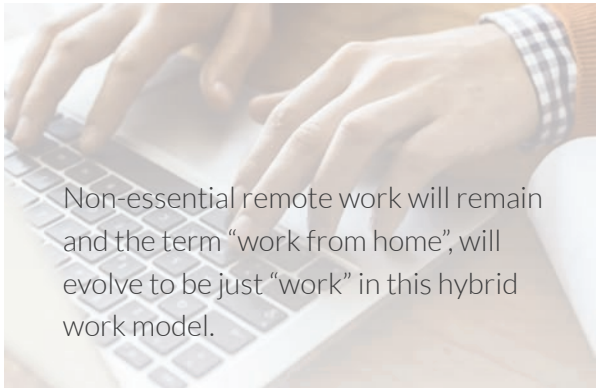
As organizations define their version of the "new normal", it's clear that things will never be the same. In fact, there will likely be many iterations of normal as we adapt to a more remote way of working, changed operations and business models, and economic impacts on our businesses.

Security operations teams must look at these changing dynamics and assess what they have done to respond to events in the first part of 2020, as well as look forward to where they should focus their efforts to manage cyber attack risk and realign with business operations and risk teams going forward.

We believe there will be five key evolutions that will emerge as security operations teams assess how to best secure the new ways of operating. These five evolutions are areas rising in importance to secure the 'new normal' as well as provide a foundation for navigating the next wave of digital transformation that organizations will undertake.

What does the “Next Normal” Look Like?

It is almost impossible to predict what the “next normal” is or will be. Each organization is impacted in different ways based on their business model, workforce and global economic factors. However, there are a few things that will be consistent for most organizations as they adapt to change.



Non-essential remote work will remain and the term “work from home”, will evolve to be just “work” in this hybrid work model.

Digital transformation will be accelerated as part of the changes in how we work.

Threats continue to rapidly evolve to take advantage of the remote workforce to exploit human and technical vulnerabilities

Security operations is giving up a sense of control allowing more users to connect to data and applications from outside a controlled environment. More direct-to-cloud access will require stronger access controls, broader visibility and a renewed focus on user behaviors and will benefit from a detection and response posture over traditional prevention approaches

Business operations will change. Security operations will need to be agile and adjust to changing C-suite priorities in investments going forward as the global economic slowdown will impact investment in IT, technology and security.

Evolution #1:

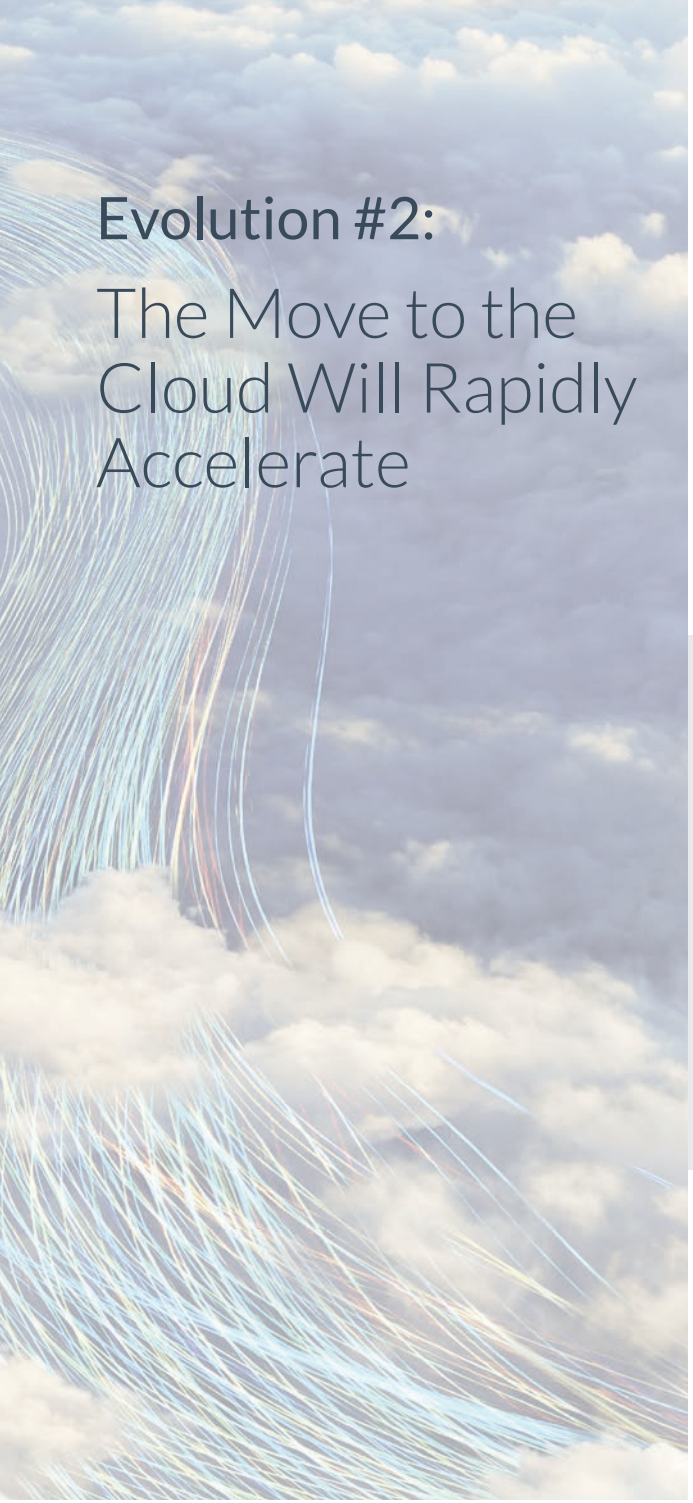
There Will Be a Lasting Change to What We Think of as the "Corporate Network"

Can organizations reduce risk by preventing some or most workers from accessing the corporate network? Is it possible to minimize the amount of traffic that traverses the corporate network as a passthrough function which in turn minimizes risk to the greater corporate environment?

This notion may seem far-fetched, but in looking at the evolution of how users are accessing vast amounts of information remotely during the pandemic through direct to cloud and SaaS resources, it's not unthinkable. There will always be some need for the corporate network but looking at how hybrid work environments will be adapted in the "next normal", it is clear that organizations may want to reassess their network and access architectures to leverage zero trust models and opportunities to reduce costs and complexity of the network environment.

Security operations and IT leaders are reassessing their environments and needs for the hybrid working model, leading them to evaluate how to:

- Implement a zero trust aligned network architecture approach to manage the changing workforce dynamics
- Reduce user access to corporate network and VPN to minimize passthrough traffic on the network
- Reassess access controls for the hybrid working model



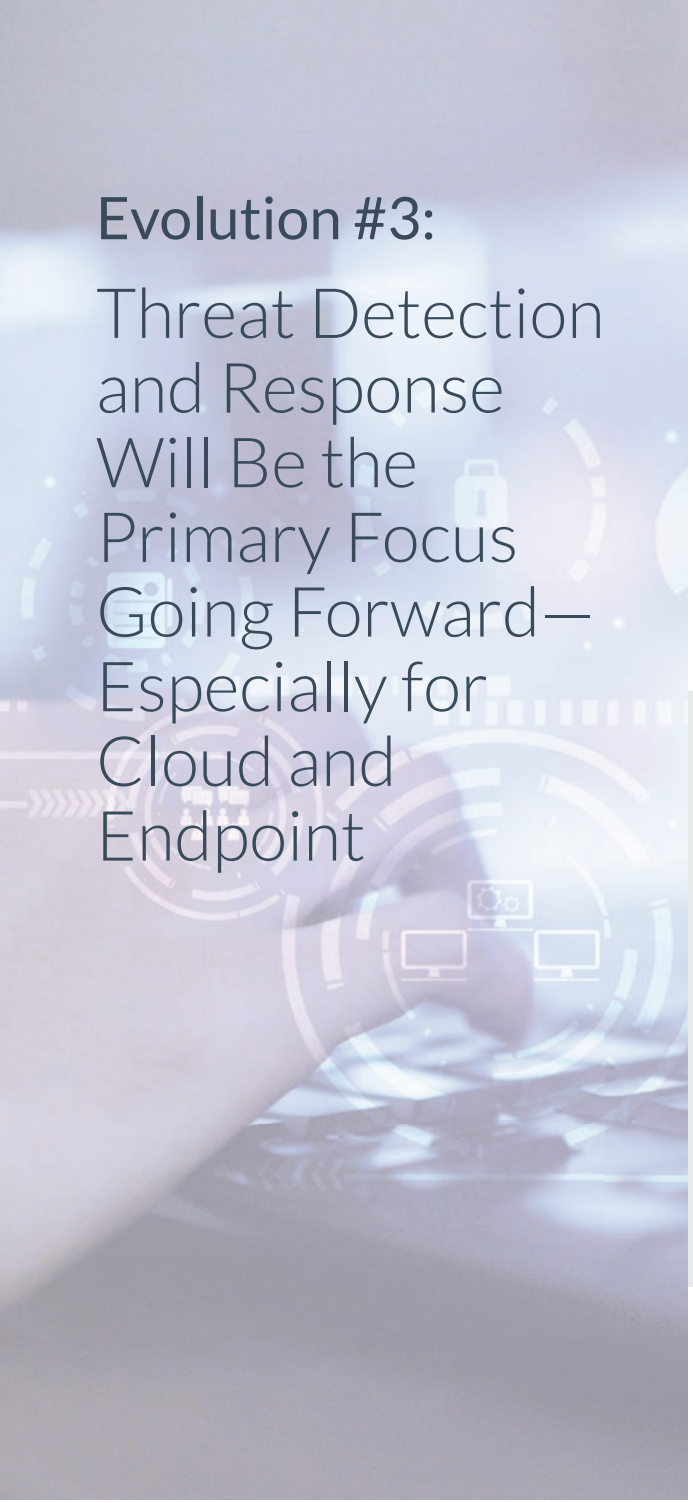
Evolution #2:

The Move to the Cloud Will Rapidly Accelerate

Digital transformations were already in full force in most organizations as they continued to adapt to the digital economy before the pandemic. Organizations that were further along their transformation journey could realize tangible benefits as they were forced to implement work from home at a speed and scale not imagined (literally overnight, in some cases). A lesson learned from the pandemic is that the need to transform to leverage the cloud isn't something that can wait. CEOs and business leaders will accelerate their cloud initiatives as a result, to either catch up or further accelerate their digital operations. While this may be tempered in the short term as economic factors play into investments, there are clear signals that investments in digital and cloud will pick up.

To adapt to growing cloud environments, security operations leaders will:

- Heighten cloud visibility as more workloads shift to cloud
- More aggressively assess third-party XaaS visibility and controls
- Move more security infrastructure and tools into the cloud



Evolution #3:

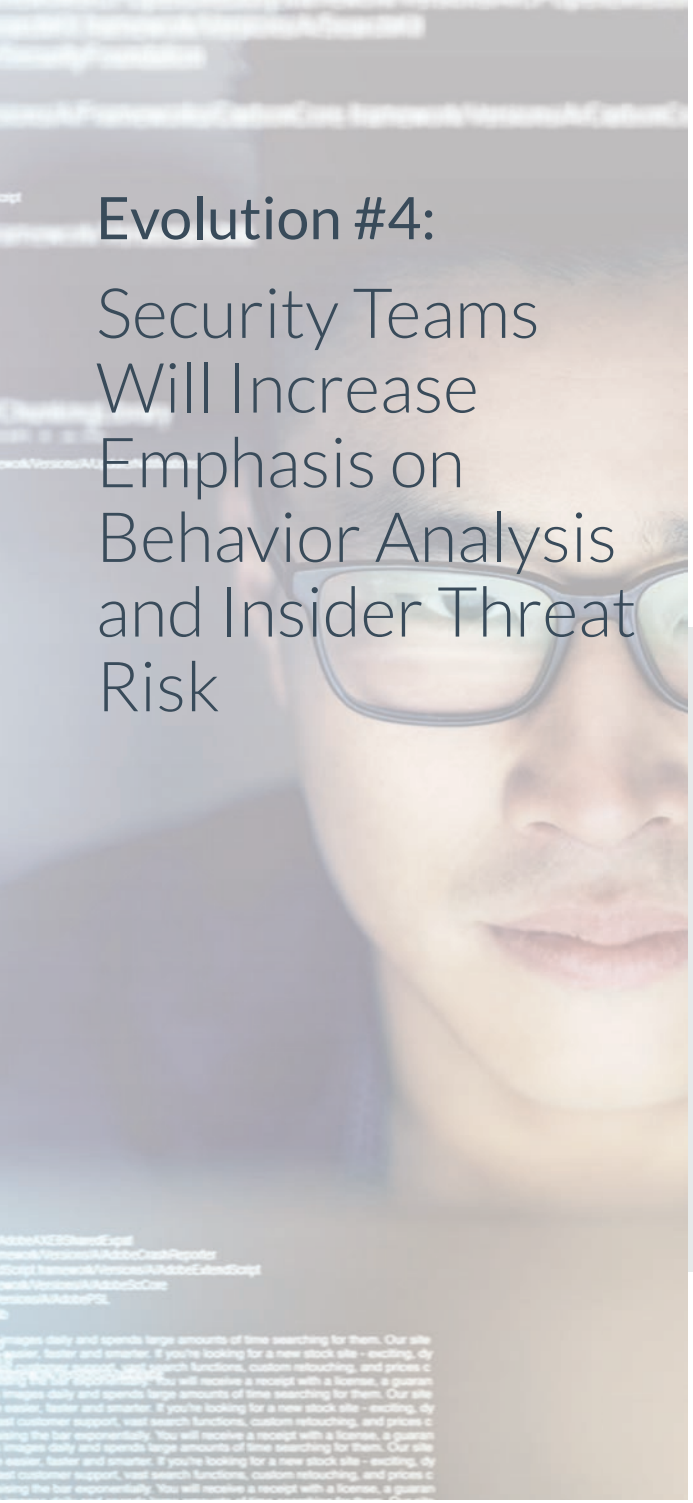
Threat Detection and Response Will Be the Primary Focus Going Forward—Especially for Cloud and Endpoint

A growing trend prior to the pandemic was the shift in traditional mindset from a prevention-oriented security posture to one rooted in the understanding that it's not possible to prevent every attack. Therefore, the push to heighten threat detection and response capabilities has evolved to detect the threat before it has a negative impact and remediate effectively.

Now, more than ever, this shift will accelerate as remote or hybrid work becomes the norm for large portions of the workforce. Explosions of endpoints at continued mass scale increase the threat surface as off-network users will assume an increased likelihood of infection. This puts the need for threat detection and response into primary focus for security teams in the near and mid-term.

Security operations leaders are investing in detection and response to:

- Ingest more from the cloud applications and services as well as XaaS environments
- Enhance packet-level visibility across the on-premises, hybrid and cloud infrastructure
- Increase endpoint detection and response (EDR) as a critical component to managing endpoint threats outside a controlled environment



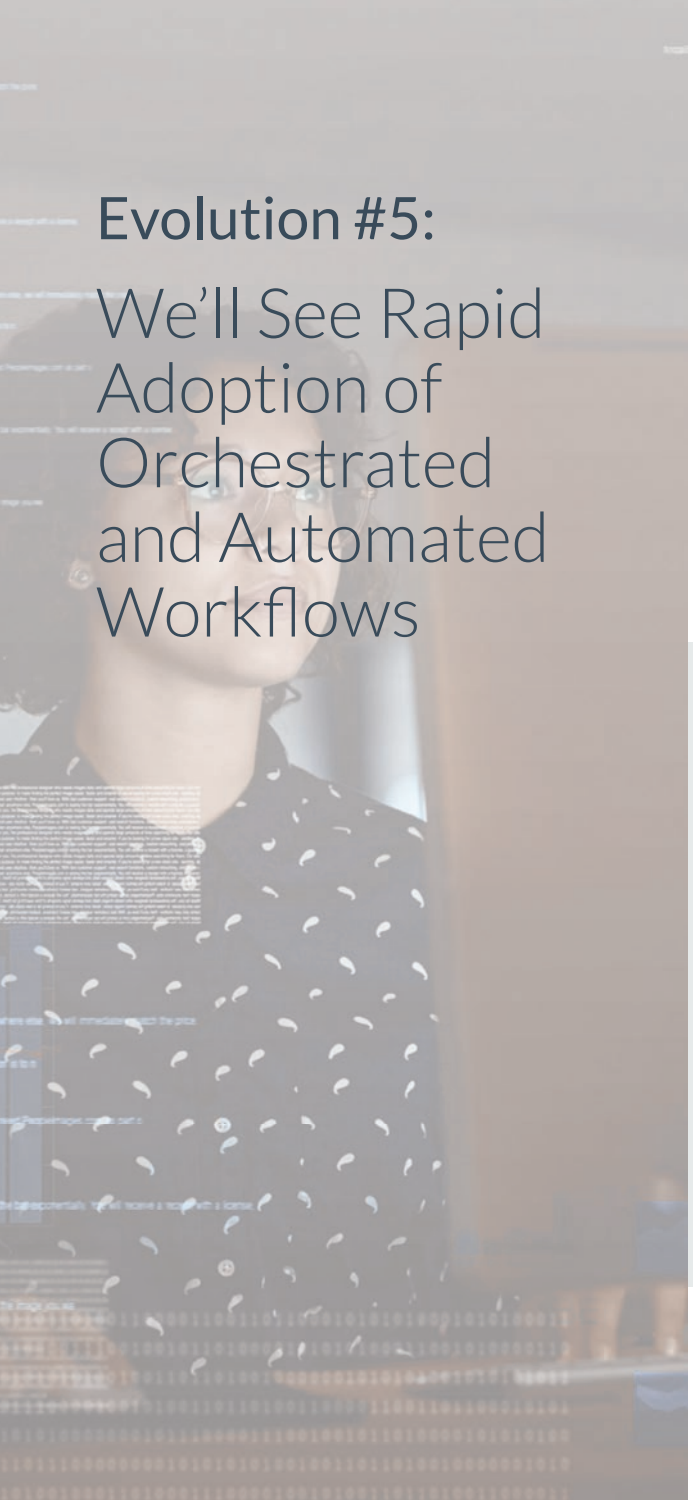
Evolution #4:

Security Teams Will Increase Emphasis on Behavior Analysis and Insider Threat Risk

Humans have always been the weakest security link. We've seen this weakness exploited during the global pandemic. Phishing attacks, fraud, ransomware, DDoS and nation-state attacks have unrelentingly targeted the workforce. As organizations embrace the hybrid work model going forward, with more users outside the traditional security controls, insider threat risk is elevated. Security teams must look at better ways to understand user behaviors across the environment and endpoints to detect anomalies. Advanced artificial intelligence with machine learning models are no longer nice-to-have, but essential in understanding behaviors and detecting the anomalies of the remote workforce.

Security operations leaders seeking to home in on behaviors more can:

- Combine behavior analysis with other signals to detect anomalies and suspicious behaviors to more quickly identify threats
- Leverage unsupervised machine learning for artificial intelligence to eliminate the need for human intervention as the system self-learns and tunes to adapt with changing dynamics
- Identify changing behavior patterns to flag insider threats more effectively



Evolution #5:

We'll See Rapid Adoption of Orchestrated and Automated Workflows

Virtualized SOCs are not new. Organizations have been enabling distributed virtual security operations for years, taking advantage of cloud-based technologies, managed service providers, remote analysts, around-the-clock detection and response, and managing costs. However, the virtualization of most of the organization, including those areas required to support threat response efforts, made it clear that without automation and orchestration tools, teams could struggle to respond to threats as efficiently. This exposed a weakness that motivated security operations teams to look at augmenting their current capabilities to enhance their ability to automate and orchestrate threat detection and response.

Security operations leaders looking to evolve should:

- Enable security operations to investigate issues working from the same central game plan regardless of where analysts are located
- Clearly identify workflows, tasks, dependencies and owners to maximize speed and efficiency
- Leverage automation tools that perform mundane or monotonous tasks, allowing the analysts to focus on what's important

We've Got You Covered—Even from a Distance

There is no way to predict the future and what the lasting impacts of the pandemic will be for organizations. What is true is that there are emerging factors that security operations leaders should be looking at to adapt to the new—or better stated, ***next***—normal. These five evolution areas can help lay a foundation for what may come while also modernizing security operation and helping organizational resiliency.

NetWitness is a strategic partner for security operations leaders to assess their current capabilities and understand where they may need to evolve to embrace what's next. Our tools, services and assessments are tailor-made help you secure the next normal and minimize cyber attack risk.

Security Operations	Permanent adjustment to what we think of as a "Corporate Network" • Reintroduction challenge—zero trust network architecture • Off-network users will assume an increased likelihood of infection and thus shift focus to detection/response	Accelerating the move to the cloud • Heightened cloud visibility as more workloads shift to cloud • Third-party XaaS visibility and controls	Increasing focus on behavior and insider threat risk • User behavior is more paramount • Changing behavior patterns to flag insider threats • AI/ML models getting better and more reliable	Threat detection and response are the focus (less preventions)—especially in cloud and endpoints • Require to ingest more from the cloud/XaaS • Packet-level visibility • EDR critical to managing endpoint threats outside controlled environment	Workflow automation and orchestration • Working from the same game plan • Tasks dependencies and owners and are identified
NetWitness Solutions	NetWitness® Platform NetWitness SecurID® Access	NetWitness Platform (cloud deployment)	NetWitness UEBA NetWitness Endpoint NetWitness Network NetWitness Logs	NetWitness Endpoint NetWitness Log NetWitness Network NetWitness UEBA	NetWitness Orchestrator

About NetWitness

NetWitness, an RSA® Business, provides comprehensive and highly scalable threat detection and response capabilities for organizations around the world. The NetWitness Platform delivers complete visibility combined with applied threat intelligence and user behavior analytics to detect, prioritize, investigate threats, and automate response. This empowers security analysts to be more efficient and stay ahead of business-impacting threats. For more information, go to netwitness.com.

NETWITNESS