aws | Deloitte.

Innovate with confidence

Embrace the full potential of cloud cybersecurity

How a robust cloud security framework allows you to push boundaries

Today, industry-leading organizations are integrating digital technology into many aspects of their business, fundamentally changing how they operate. They leverage advanced technologies to help create competitive advantage: devising radically new customer experiences, empowering global workforces, streamlining complex supply chains, and revolutionizing product development. They also take advantage of the scale, flexibility, and cost-effectiveness of cloud platforms and the latest developments in mobile computing, big data analytics, generative artificial intelligence (AI), and other fields.

But innovation and risk go together. When you increase interaction with customers, suppliers, and other parties and widen collaboration among your employees, you create a vastly larger "attack surface." Your cybersecurity teams are tasked with monitoring and defending exponentially more systems and devices, in more places, processing more confidential information. You need to detect and monitor the activities of increasingly sophisticated threat actors, including ransomware gangs, fraud rings, nation state-funded hacking teams, and more. You also may need to comply with rigorous government regulations and industry standards for information security, privacy, and governance.

The tension between game-changing technologies and an expanding attack surface creates strategic business value and unprecedented risk.

With strong cybersecurity practices throughout your organization, you can:

- Deploy innovative technologies and business processes faster, with confidence.
- Establish positive reputations with customers, business partners, regulators, and investors.
- Reduce the cost of managing and protecting information systems and data.

Conversely, if your organization doesn't progress beyond legacy cybersecurity paradigms, you run the risk of slower innovation, impaired reputation, and higher costs.

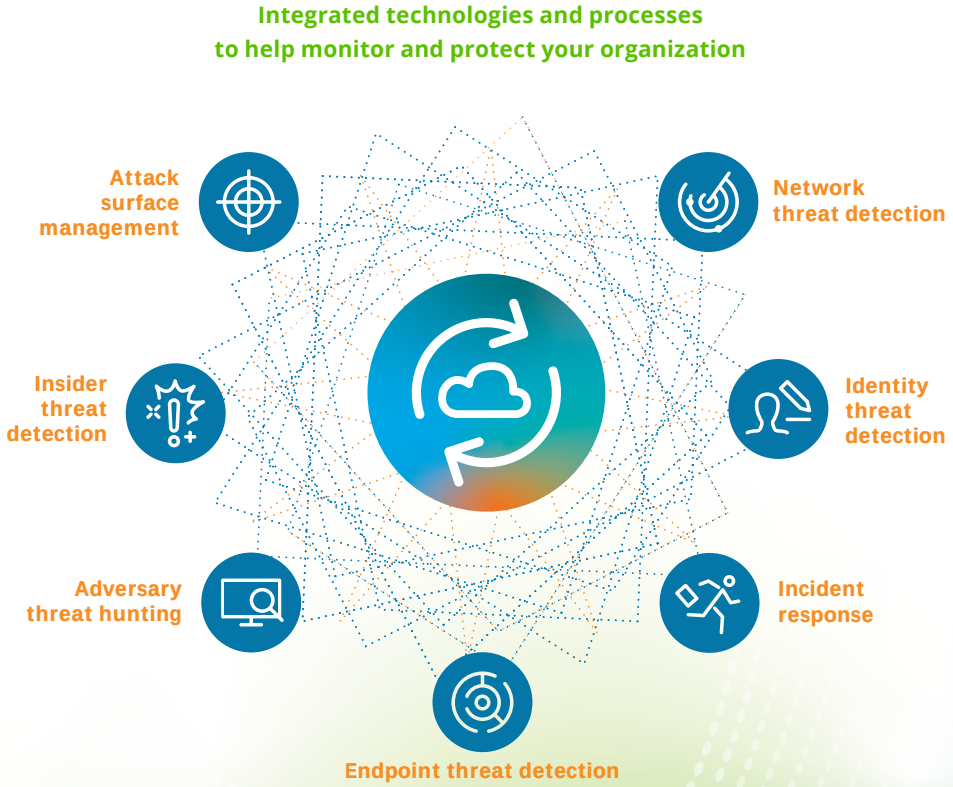
The tension between game-changing technologies and an expanding attack surface creates strategic business value and unprecedented risk.

Digital transformation demands cybersecurity

To make cybersecurity a competitive advantage, your organization should consider adopting an end-to-end approach to cybersecurity that:

- Provides security and helps address compliance by design for cloud transformation, from ramp up to operationalization.
- Brings together an integrated, cohesive set of cybersecurity services and products and offers access to specialized resources and managed services.
- Eliminates data silos to deliver enterprise-wide visibility into vulnerabilities and threats.
- Helps anticipate and prevent attacks on cloud infrastructure and applications and enables you to respond and recover faster.
- Leverages threat intelligence shared from thousands of peer organizations and specialized cybersecurity firms.
- Makes it easy to take advantage of advanced cloud platforms and powerful AI-driven analytics.

Let's examine how a robust cloud security framework can allow you to embrace the full potential of cloud cybersecurity and innovate with confidence.



Monitor and protect through enterprise-wide readiness

Growing organizations need multiple advanced technologies and integrated processes to help monitor and protect their ever-expanding attack surface.

However, your organization probably doesn't have the time to select, implement and integrate all the required detection and response tools. You also may not have enough cybersecurity professionals to continuously monitor your diverse cloud and data center environments, analyze and triage alerts, and respond expeditiously to attacks. That's why you might want to follow the example of the many organizations that have turned to a managed service provider with the experience, infrastructure, and experienced cybersecurity teams to manage and staff a comprehensive, robust cloud security platform.

Visibility and AI-driven analytics

Enterprises now produce vast quantities of cybersecurity-related data that can be used for threat detection and incident response, including millions of daily logging events. Unfortunately, most of that data is in isolated files scattered across the enterprise and its cloud platforms, and there is far too much for any human to analyze.

With the right cybersecurity strategy, your organization can leverage unprecedented volumes of cybersecurity data to supercharge your threat detection, incident response, fraud detection, adversary threat hunting, and digital forensics capabilities. You can accomplish this with a cyber analytics engine that ingests logs and security data from cloud platforms, enterprise applications, endpoints, and security and network devices, then uses AI to help identify patterns, uncover new and previously unknown threats, detect anomalous activities and policy violations, and provide context and recommendations for security teams.

Incident response and recovery: Preparation, plans, and playbooks

Today, the ultimate success of many cybersecurity programs depends on an organization's ability to respond to attacks, quickly contain them, and rapidly return to normal business operations. Investing in these areas is critical for safeguarding data and systems. A slow or incomplete response can lead to unwanted media attention, loss of reputation, data breach notification costs, and business disruption.

Your organization can take an integrated approach to cybersecurity by systematically assessing risks and developing an incident response program customized for your organization's business, strategy, and structure.

The elements of that program should include:

- Tailored cyber monitoring activities
- Determination of incident response and recovery priorities
- Policies and resources for effective alert triage, threat analysis, and forensics
- Documented plans and playbooks for near-term attack containment and rapid recovery and resumption of normal operations

Today, the ultimate success of many cybersecurity programs depends on an organization's ability to respond to attacks, quickly contain them, and rapidly return to normal business operations.

Enterprise cloud transformation and cloud management

An end-to-end approach to cybersecurity facilitates security and compliance by design for cloud transformations. This includes activities to manage cloud infrastructure, regulatory compliance, and cyber risk in the cloud.

For example, your organization should have a well-designed plan to guide the transition of applications to cloud platforms and services. This includes learning how to manage security capabilities using cloud-native tools for vulnerability scanning, firewall configuration and management, and patch management. You should also get up to speed on managing and collecting logs for operating systems, network and security devices, and cloud platforms. And of course, you will need to understand compliance requirements for cloud environments and be able to monitor compliance as your cloud environment evolves.

Another critical part of the transition is upgrading to advanced identity and access management practices. That includes providing functions such as single sign-on (SSO), multi-factor authentication (MFA), and role-based resource provisioning. You will also need to be able to enforce encryption and secrets management policies.

Finally, if your organization is creating its own cloud-based applications, you will want to make sure that your development teams truly master DevSecOps processes and practices.

Shared threat intelligence, AI, and autonomous security

For decades, cybersecurity teams played catch-up with threat actors who leveraged the latest technologies and zero-day attacks to catch defenders unprepared. Now, you have an opportunity to turn the tables on threat actors by using widely shared threat intelligence, AI, and big data analytics to help anticipate attacks before they reach their goal—and possibly before they really get started.

Threat intelligence gives your cybersecurity teams visibility into the tactics, techniques, and procedures of cybercriminals, ransomware gangs, hacking groups, and other threat actors. These include the tools they use, the phishing emails they send, the vulnerabilities they exploit, the assets they target, the indicators they leave on endpoints and networks, and their servers and infrastructure on the internet. When threat intelligence is shared widely and rapidly between enterprises, government agencies, and cybersecurity firms, it can help you anticipate and block the attacker's next moves.

AI and big data analytics provide transformative capabilities. By centralizing and normalizing data into a flexible "data lake" on a scalable cloud platform with sophisticated AI models to detect patterns associated with threat activity, you can obtain new capabilities that detect indicators of attack, compromised endpoints, lateral movement by threat actors, and anomalous activities on networks and cloud platforms. AI can also be used to help pinpoint vulnerabilities, misconfigurations, insecure application code, over-privileged user accounts, and other security weaknesses that in the past have given attackers access to networks, applications, and data stores.

When these transformative technologies are used at their highest level, they can enable autonomous security, where attacks can be detected, analyzed, blocked, and remediated with minimal human intervention—turning the tables on threat actors.

Accelerate your cloud journey with ConvergeSECURITY

ConvergeSECURITY combines the power of Amazon Web Services (AWS) technology with the cybersecurity capabilities of Deloitte to accelerate cloud initiatives and digital innovation. It delivers the flexibility, scalability, and cost optimization of a cloud-enabled IT infrastructure, while integrating a seamless set of cybersecurity services.

The ConvergeSECURITY services suite:

- Provides 24/7 security protection and monitoring of essential resources.
- Delivers actionable security threat intelligence across your organization's digital estate.
- Leverages a combination of AI-enabled cloud security and compliance product solutions, consulting experience, and tailored resources.
- Centralizes data and increased threat intelligence throughout your organization to effectively detect, respond to, and recover from sophisticated cyber threats.

Benefits of this joint solution include:

Eliminating data silos

AWS services, including Security Lake, that are integrated by Deloitte in the Cyber Analytics and AI Engine solve the siloed data challenge across your digital estate. ConvergeSECURITY also delivers data aggregation and out-of-the-box data integration of security products, helping you unlock the power of your security data.

Generating actionable insights

Deloitte and AWS collaborated on the Cyber Analytics and AI Engine to deliver insights that reduce risk and enable cybersecurity automation to accelerate prevention, detection, response, and recovery. Underlying AWS infrastructure powers AI and Machine Learning models developed to help predict ransomware campaigns, look for lateral movement, find Zero Day threats, and identify anomalies before they become bigger issues.

Being able to anticipate and prevent attacks

An integrated security approach allows threat detection analytics to be fed by high quality, shared multi-lateral data. When more data is contributed, the effectiveness of analytics and machine learning increases, generating more accurate threat detection to anticipate and prevent attacks.

Faster response and recovery

You're better able to safeguard data, systems, and reputation when you have response and resiliency plans prepared before a cybersecurity incident occurs. This includes being able to recover mission-critical business functions from cloud back-ups if a breach happens, so you can restore capabilities and services.

Contact us

Our goal is to provide autonomous security that has human oversight but requires minimal intervention. Let's talk about how we can make this a reality for your organization.

Julie Bernard
Global ConvergeSECURITY Leader
Deloitte & Touche LLP
juliebernard@deloitte.com

PJ Hamlen
Worldwide Leader, Global Partner Security Initiative
AWS
pjhamlen@amazon.com

www2.deloitte.com/us/convergesecurity

Deloitte.