accenture

# Emerge stronger with adaptive security

## Take steps for a more flexible and secure future

June 2020

NOW NEXT

# OUTMANEUVER UNCERTAINTY

As the health and humanitarian impacts of the COVID-19 pandemic evolve, so do the business and economic challenges. Organizations looking to balance their immediate needs with longer-term opportunities will see the trade-offs play out across three waves of impact: the Now, the Next and the New Normal.

The Now includes an emphasis on supporting people, customers and suppliers. The Next will feature refocusing the business to withstand new threats and seize new opportunities. And the New Normal will require navigating rapid shifts in cultural norms, values and behaviors.

This is the moment to reinvent business models and reintegrate the value organizations provide into a new societal landscape. The time to shape a mind-set of bold business transformation powered by new approaches to technology and responsible leadership is underway.

# Security challenges

Operational resilience is fast becoming a key business metric across industries.[1] Security teams are used to responding to constant threats and continuous change. Every day, they defend their organizations against new or existing adversaries whose aims are to steal, deceive or disturb business operations.

Everything has changed. For C-suite executives, daily conversations about operations and profits now include business survival, safety, security and resilience. Further, working from home has opened up new attack vectors and workforce challenges—including those from insider threats.

Security leaders are well placed to make the practical changes that keep their organizations safe and secure and help people adapt to new ways of working that improve security in the long term. But they must adapt in two ways. First, they must bring their existing focus on business risk and resilience into the broader executive planning discussions. Second, they must take steps to build a new, more resilient business from the ground up.

**Security leaders are in pole position to act as key influencers.**

## Challenge 1

Organizations are rethinking their culture, collaborative practices, and the technology necessary to enable distributed working environments at scale—but while some changes are short term, they must prepare to outmaneuver uncertainty in the future.

## Challenge 2

Malicious threat actors are taking advantage as organizations reconfigure their vulnerable supply chains, offer more digital experiences, and meet the growing demands of a remote workforce.

## Challenge 3

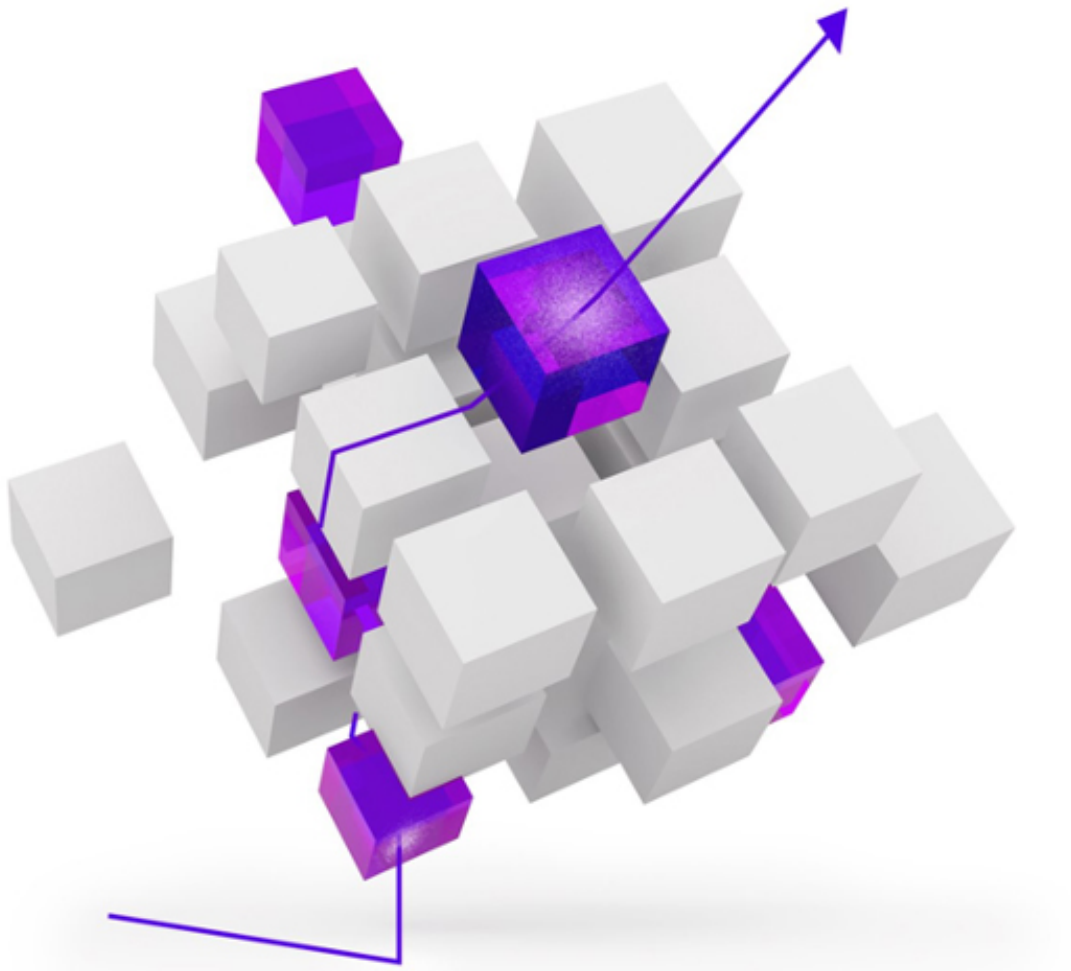
Security leaders must adapt to service new business priorities and evolve how they detect, defend and recover from threats in the face of unprecedented demands.

# Where are we now?

Cyberattackers are preying on the susceptibility of newly remote workers by offering lures and traps that imitate credible sources.

Security Operations Centers need to tap into tactical, operational and strategic threat intelligence to identify trends and technologies that threaten business continuity.

**In these difficult times, security leaders have an opportunity to reimagine their strategy and technologies from the ground up.**



# Understanding risks

## Five fundamental questions can determine how to best protect the work environment:

### Who is a potential threat?

Cybercriminals who have attempted breaches before will most likely try again. Bear in mind, new threats are constantly emerging—for instance, as nation-states try to exploit work-from-home environments [2].

### What are the logical threat vectors?

Take account of the thousands of coronavirus-related domain names emerging since January 2020, creating new opportunities to breach cybersecurity defenses [3].

### What is the impact of disinformation?

As people seek information, threat actors attempt to take advantage of confusion and uncertainty to penetrate cyber defenses.

Communicating first can help disinformation lose its power.

### Where are your vulnerabilities?

Ask what concrete steps the enterprise can take to enhance cybersecurity in the current environment. Recognize budgets may be affected almost immediately and plan accordingly.

### How can you build a more resilient business?

Factor into the future the additional security vulnerabilities and cultural support necessary for remote working, the importance of digital identity and authentication, and the data, tools and techniques needed to mitigate new challenges for enterprise monitoring.

# Act now



As organizations stabilize their current operations, security leaders can put the right controls in place to create a safe and secure working environment for their enterprise. Here are four elements of adaptive security* which apply now:

## 01
## Secure mind-set

**Prioritize the human factor**

Security leaders continue to play a role in maintaining the health and well-being of the workforce, which is essential for the smooth running of the enterprise and helps to mitigate risks to the larger community.

## 02
## Secure network access

**Protect the company infrastructure**

Security leaders can inform employees about known vulnerabilities and make sure their teams are diligent when it comes to testing and intelligence.

## 03
## Secure work environments

**Be brilliant at the basics**

With workforces now remote, security leaders need to shift the information security focus from an enterprise infrastructure to a virtual and cloud environment.

## 04
## Secure collaboration

**Provide the tools and the teams to tackle risk**

Security leaders are well-placed to evaluate and promote solutions that mean distributed teams can connect and collaborate safely, securely and effectively—helping their organizations to create better employee experiences while making them more productive.

*See Appendix page 10 for more on these four elements

# Act next



Decisions on how organizations operate in the near term have a knock-on effect on how they will operate in the future. As COVID-19 restrictions on the social and business activity are revised or lifted, it's time for organizations to think more broadly about their approach to security.

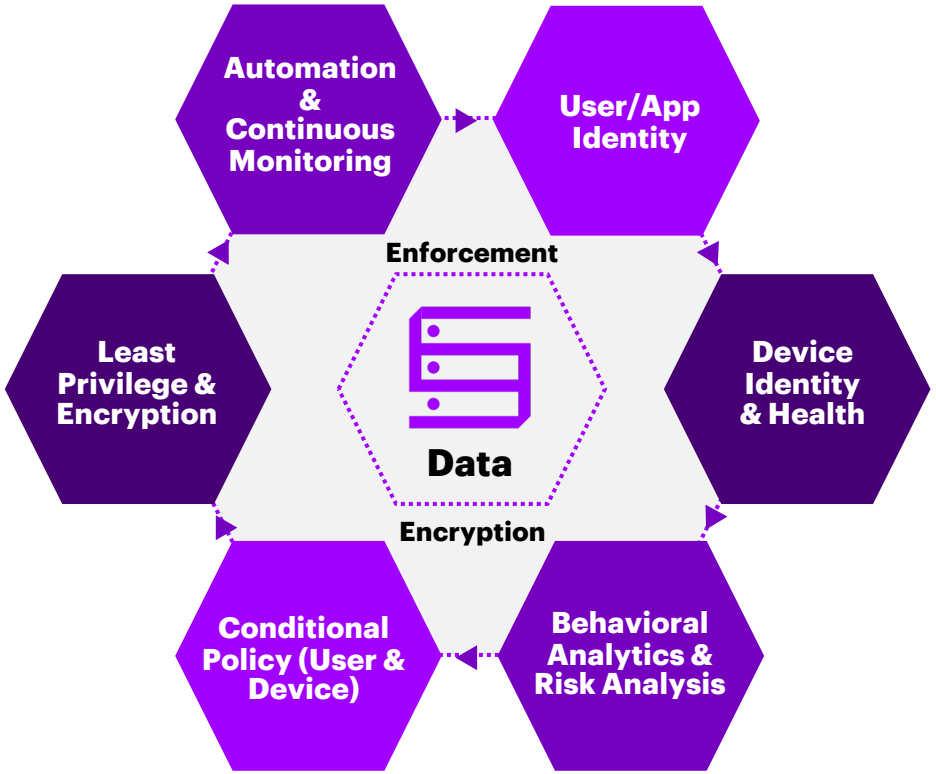
Adaptive Security enables organizations to provide a secure and smooth experience to continue operations. Security leaders can reinvent access by using cloud-based solutions to meet the increased demand for a fast, frictionless and secure remote access to enterprise data and applications.

The use of a zero-trust framework for authentication helps protect remote access using a strong authentication that includes multifactor authentication, adaptive authentication, fraud prevention, identity proofing, behavioral analytics and biometrics, and device telemetry.

Empowered employees can collaborate better and protect the company data—but trust must be balanced with vigilance. Security professionals can help by providing simulations to stress-test existing processes, while penetration testing and red teaming can also be used to identify gaps or areas for improvement.

**Rapidly deploying a zero-trust framework with built-in technologies can enable secure remote access without relying on traditional virtual private network (VPN) solutions.**

## ADAPTIVE SECURITY—A ZERO-TRUST MODEL



# Emerge stronger

Security practices that serve today's needs, as well as the future's, need security leaders and their organizations to:

**01 THINK "ANYTIME, ANYWHERE"**
Secure all users, devices, and network traffic consistently with the same degree of effectiveness, regardless of where they are based. Remember that secure network access and applications are just as fast with security as they are without—if not faster.

**02 BE TRANSPARENT**
Give users access to what they need when they need it. Make these changes transparent to them—without asking them to "jump through hoops" to do their job effectively.

**03 INSPIRE CALM AND CONFIDENCE**
Security leaders can be the catalyst for change, using empathy and compassion to deliver a more agile response. Employing adaptive security creates confidence; for instance, organizations can use the cloud or expand access to more remote users.

**04 WHERE POSSIBLE, SIMPLIFY**
Consider managed services and automate where it makes sense. For instance, security event response, tool deployment, and rule management, can benefit from limited human intervention.

**05 BUILD FOR RESILIENCE**
As organizations look to emerge stronger, business continuity and crisis management plans must be fit for purpose. Engage with business leaders to plan, prepare and practice for greater cybersecurity resilience, backed by the right resources and investments.

NOW NEXT

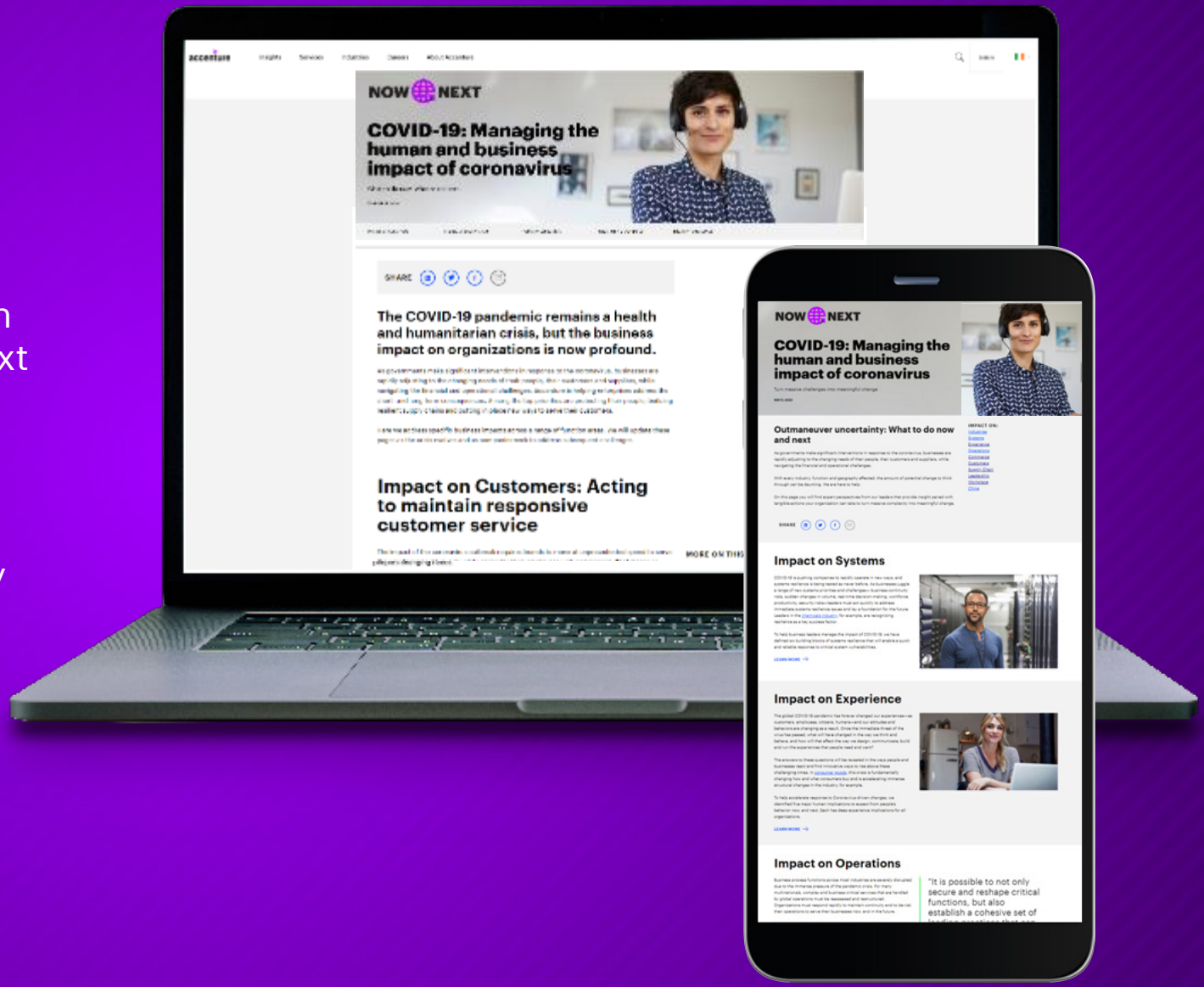
**Accenture believes a multi-dimensional crisis management strategy, with many work streams and teams that collaborate closely, often on a daily basis, is the answer to security resilience—and can help to protect people from harm.**

To help our clients navigate both the human and business impact of COVID-19, we've created a hub of all of our latest thinking on a variety of topics.

Each topic highlights specific actions which can be taken now, and what to consider next as industries move toward a new normal.

From leadership essentials to ensuring productivity for your employees and customer service groups to building supply chain resilience and much more, our hub will be constantly updated. Check back regularly for more insights.

VISIT OUR HUB HERE



# Appendix

## An action list to help react and stabilize now

As organizations stabilize their current operations, security leaders can put the right controls in place to create a safe and secure working environment for their enterprise. Here are four elements of adaptive security which organizations can adopt now:

### 1. SECURE MIND-SET

#### Prioritize the human factor

Security leaders continue to play a role in maintaining the health and well-being of the workforce, which is essential for the smooth running of the enterprise and helps to mitigate risks to the larger community.  Security leaders should:

- Be pragmatic and collaborative to better support a remote workforce. Quickly educate users on the potential risks of remote work, including phishing or the use of unsanctioned Software-as-a-Service (SaaS) applications for collaboration.
- Instill a "security first" ethos among employees by keeping them up-to-date with company information protection procedures, including those regarding hard drives and file encryption in storage and in transit. Some element of compromise may be needed, such as employees using personal devices in certain circumstances or as an interim measure. Make sure that computers and devices include the most current system and application versions.
- Factor in the human side of maintaining continuity of operations. People are dealing with personal fears and hardships which need to be handled sensitively and supportively. For example, schools closing can have a significant impact on employees' ability to be productive. Also, work with other business leaders to award recognition, where due, to improve well-being and engagement across teams—both locally and globally—which contributes to maintaining business continuity.[4]
- Be empathetic and available to their teams. Use company-approved broadcast video to discuss the situation and actions that your organization is taking to protect your people, and to enable them to work with minimal disruption.[5]

# Appendix

## 2. SECURE NETWORK ACCESS

### Protect the company infrastructure

Security leaders can inform employees about known vulnerabilities and make sure their teams are diligent when it comes to testing and intelligence. Security leaders should:

- Carry out penetration testing to assess existing secure remote access capabilities, including bandwidth or user constraints, and complement existing solutions with cloud-based secure connectivity that can be deployed in days.
- Take advantage of threat intelligence to identify common Tactics, Techniques and Procedures (TTPs) and threat actors' methods for targeting remote employees accessing company networks. Train your workforce to identify these early warning signs.
- Recognize that remote working relies on home WiFi routers and VPN connections to the company infrastructure and could bring about misconfigurations which risk the leakage and theft of sensitive company information. Educate employees on home network best practices by:
    - Planning fallback measures for phone-based and off-net communications and work, as many VPN providers may experience issues with the large influx of users joining the network.
    - Reminding employees to change the default administrator password on their router so it is strong and unique, enable WPA2 or WPA3 on their routers to encrypt online activity, and create a strong network password. They should also turn off network discovery and folder sharing when connecting to a new network.
- Investigate VPN solutions or other asset management solutions that enable inventory and patch distributed systems and endpoints.

# Appendix

## 3. SECURE WORK ENVIRONMENTS

### Be brilliant at the basics

With workforces now remote, security leaders need to shift the information security focus from an enterprise infrastructure to a virtual and cloud environment. Security leaders should:

#### 3.1 Secure virtual desktops

- Invest in and deploy an endpoint detection and response tool (EDR). Build in analytics and automation to reduce the amount of human intervention required and better protect multiple devices in less secure locations. Introduce clear governance (definition of access, provisioning/deprovisioning, controls for segregation of duties and recertification) to reduce the attack surface and limit the opportunity for errors and malicious actors.
- Introduce secure virtual desktop solutions, such as Citrix, to avoid exposure to the public Internet for use on unmanaged devices without two-factor authentication or properly secured desktop images.

#### 3.2 Secure managed personal devices

- Be aware that new bring-your-own-device (BYOD) solutions may create security risks. Existing patching/update infrastructure may assume devices are on-premises or managed.
- Use threat intelligence to identify whether credentials have been harvested, or if threat actors are selling access in the Deep Web and Darknet.

#### 3.3 Secure policy-based access

- Put in place privileged access management for high-impact access (increased security such as password rotation, session recording and analytics around privileged access) to reduce the risk of a privilege escalation from an attacker coming in via your remote access route. Introduce policy-based access which creates “all or nothing” access to SaaS applications requiring fully managed devices to access without risk. Implement advanced access management (risk based and multifactor authentication) to reduce the risk compromise with the access provided.

# Appendix

## 4. SECURE COLLABORATION

### Provide the tools and the teams to tackle risk

Security leaders are well-placed to evaluate and promote solutions that mean distributed teams can connect and collaborate safely, securely and effectively—helping their organizations to optimize the employee experience while maximizing productivity. Security leaders should:

- Adopt and measure collaboration with the large-scale deployment and use of collaboration tools and through providing targeted, prescriptive guidance on how to be safe and secure when working remotely. Establish clear guidelines on how to share information securely based on data classification, audience and content type.
- Make the best of leading practices while accepting that not all work can be done remotely. Adjust expectations accordingly, both within the organization's teams and across the ecosystem of stakeholders.
- Be nimble and innovative with the latest technologies. Clearly communicate which officially approved software and tools may be used for remote working—including those for file sharing, video conferencing, virtual whiteboard collaboration and chatting.
- Anticipate the increase in volume and load from the use of collaboration tools from more employees working remotely, while also improving usability and productivity. Encourage large-scale virtual sessions using interactive broadcast and web conference platforms to support the shift from physical to virtual workshops and conferences.

# Contacts

**Kelly Bissell**
Senior Managing Director
Global Lead
Accenture Security
kelly.bissell
@accenture.com

**Ryan LaSalle**
Managing Director
North America Lead
Accenture Security
ryan.m.lasalle
@accenture.com

**Paolo Dal Cin**
Managing Director
Europe Lead
Accenture Security
paolo.dal.cin
@accenture.com

**Andrew McLauchlan**
Managing Director
Growth Markets Lead
Accenture Security
andrew.mclauchlan
@accenture.com

**David Fitch**
Managing Director
Accenture Security
david.fitch
@accenture.com

**Wayne Mattadeen**
Managing Director
Accenture Security
wayne.o.mattadeen
@accenture.com

# References


1. Productivity in Uncertain Times through the Elastic Digital Workplace, Accenture, March, 2020. https://www.accenture.com/us-en/about/company/coronavirus-solution-elastic-digital-workplace

2. Communication is the answer to cyberthreats in a crisis, Accenture, April, 2020. https://www.accenture.com/us-en/blogs/cyber-defense/communication-is-the-answer-to-cyberthreats-in-a-crisis

3. Ibid.

4. Continuity in Crisis: How to run effective business operations during the COVID-19 pandemic, Accenture, April, 2020. https://www.accenture.com/us-en/insights/operations/coronavirus-effective-business-operations

5. Productivity in uncertain times through the elastic digital workplace, Accenture, March, 2020. https://www.accenture.com/us-en/about/company/coronavirus-solution-elastic-digital-workplace

# About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 509,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives.

Visit us at **www.accenture.com**

# About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence.  Follow us @AccentureSecure on Twitter or visit us at www.accenture.com/security.