

A woman with dark hair and glasses is shown in profile, looking upwards and to the left. She is wearing a dark zip-up jacket. The background is dark with red, glowing lines of code or data flowing across the screen, creating a sense of digital activity and security.

5 Attributes of a Modern Security Program

Insight[®] 



Table of contents

A brief orientation	1
Full visibility	2
Comprehensive governance	3
Strategic identity and access management	5
Automation and streamlined workflows	6
Effective tools and skilled resources	7
Look to trusted sources.....	8



A brief orientation

As data continues to grow exponentially, there is also a rise in those looking to gain from malicious attacks. Now more than ever, it is critical for organisations to evaluate their security strategy.

In just the first half of 2021, there were

1,767 breaches reported,

resulting in the exposure of
more than 18.8 billion records.¹



The average cost was

\$1.07 million higher

in breaches where remote work was
a factor in causing the breach.²

The average total cost of a data breach —

\$4.24 million.²

At times like these, it's helpful to take a step back. What should a security program aim to do? Which goals are realistic — and which goals are not? How should security investments be made and measured?

We believe there are five key attributes to a successful and modernised security program, for any type or size of business.

¹ Risk Based Security. (August 2021). 2021 Mid Year QuickView Data Breach Report.

² Ponemon Institute. (2021). 2021 Cost of a Data Breach Report. Sponsored by IBM Security.

CHAPTER 1

Full visibility

IT environments are expanding. We're seeing growth in data volumes, device counts, platforms, and traffic. Each expansion introduces new threat vectors and additional challenges in terms of visibility.

Fact:

Worldwide data creation will
grow from 64.2 ZB in 2020 to 180 ZB by 2025.³

Consideration:

How will all of this data be monitored and secured,
particularly as it moves throughout IT environments?

Fact:

There will be more than 41 billion Internet of Things (IoT) devices by 2027, up from about 8 billion in 2019.⁴

Consideration:

What level of visibility can we reasonably aim for,
considering this level of growth in connected devices?

Fact:

87% of companies adopted or began adopting a multicloud
(using more than one public cloud provider) approach last year.⁵

Consideration:

How do you make visibility easy, or even possible,
with multiple platforms of different types in the same IT environment?

Yet, having full visibility is critical. When an IT environment provides quality visibility and activities are being monitored, many benefits can be realised.

For one, attack attempts can be thwarted, and potential damage, mitigated. A successful attack typically begins by exploiting one vulnerability, and then penetrates throughout multiple systems, from that single starting point. If a breach is detected earlier, the extent of the loss can be better controlled. In 2019, the average time to identify a breach was 206 days.² Imagine the number of records, systems, and users a cyberattacker could reach over the course of more than six months — it's uncomfortable to think about.

Visibility, paired with monitoring and/or threat intelligence tools, also contributes largely to the effectiveness of prevention efforts. User behavior tends to be patterned, moving in logical and repetitive ways. Unusual activities or movements can signal the presence of malicious actors, helping IT security managers prevent attacks and make access or policy changes that can address security gaps previously unnoticed.

³ Statista. (May, 2022). Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025.

⁴ Newman, P. (March 2020). The Internet of Things 2020. Business Insider Intelligence.

⁵ Marketpulse Research by IDG Research Services. (February 2020). The State of IT Modernisation 2020. Commissioned by Insight.



CHAPTER 2

Comprehensive governance

Many may think of frameworks like COBIT or ITIL when thinking of governance. At a high level, governance is about the ways IT decisions are aligned with business objectives or needs. Governance should also address ownership and accountability — who is responsible and who the stakeholders are.

Governance is critical for security as it helps organisations to:



Define and align around security objectives



Select and validate security solutions



Organise training, guidelines, and other user security programming



Bring security into conversations about platform adoption, networking architecture, and other components of IT strategy



Improve security posture through defined roles and processes



Effective governance can be difficult to achieve, however. In the latest Insight-commissioned IDG survey, respondents reported that the top IT modernisation challenge is establishing new governance strategies and processes to support IT modernisation and cloud.⁵

One difficult aspect of devising effective governance is, in fact, the increased use of the cloud. Organisations may have had working governance frameworks in place for years, which only addressed the data center and its clearly defined perimeter.

According to the Flexera 2022 State of the Cloud Report

89% of organisations have adopted a multicloud strategy,
and
80% are taking a hybrid cloud approach by
combining the use of public and private clouds.⁶

Extending traditional governance to the cloud is essential, yet not formulaic, and does require investments of time and resources.

This has repercussions for cloud security, or the perception of it, at least. The IDG survey found that managing public cloud security is the number-one challenge when optimising cloud experience and outcomes, closely followed by governance and process challenges.⁵

By establishing comprehensive governance, inclusive of all platforms, roles, stakeholders, etc., an organisation can ensure its security operations stay robust, relevant, and supported.

⁶ Flexera. (2022). 2022 State of the Cloud Report.

CHAPTER 3

Strategic identity and access management

Everyone and every system that lacks malicious intent does, or should, have an identity and specific access privileges. As IT environments sprawl, and endpoints proliferate, identity and access management is becoming a central topic of security conversations.

Most organisations have Active Directory® and have used various third-party services. This results in multiple identities, systems, and solutions — and a lot of complication, particularly when manual efforts are required to manage it all.

Here are several considerations to make with identity and access management, where security is concerned:



Think about the data.

How sensitive is it? Who really needs access to it? When, and for how long? What is the initial point of contact, and is this the best option? Organisations may need to pursue a data classification initiative as a first step.



Think about your users.

Have you established user types? When did you last review permissions? How are you verifying identities and granting access? From defense in depth to zero trust, there are many viable models.



Think about authentication.

Passwords are falling out of favor, fast. What alternatives have you considered? Would mechanisms such as biometrics work for your organisation? How might you transition from your current authentication approach to a more secure one in the near future?

For identity and access management to be strategic and successful, organisations should maintain all identities in a single repository, consider implementing a Cloud Access Security Broker (CASB) solution, and implement a layered security approach.





CHAPTER 4

Automation and streamlined workflows

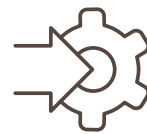
Security has no mulligans. Vulnerabilities or gaps may be exploited at any time. Human errors that lead to successful attacks are not a forgivable matter. In security, mistakes are costly. Ironically, avoiding such costs can also be quite costly, depending on the approach you take.

What do we mean? Security Operations Centers (SOCs) need to be modernised, inclusive of tool sets, technologies, processes/methodologies, and resources. In “The State of IT Modernisation 2020” survey, 57% of respondents said that upgrading security infrastructure and processes was a top obstacle to pursuit of modernising the IT operating environment.⁵ But, where in-house resources are scarce, organisations need to find external partners that can bring automation and other expertise that is critically needed.

Automation within the SOC delivers clear benefits:

- Faster detection, response, and remediation capabilities
- Fewer errors as a result of manual efforts
- Security resources freed up for strategic priorities
- Better user experiences and satisfaction

Some tasks are particularly well suited for automation. Take responding to alerts, for example. In a study by CRITICALSTART, 70% of respondents said they investigate more than 10 alerts each day, which each take more than 10 minutes to investigate (figures that were 45% and 64% higher than the previous year, respectively). Alert fatigue is a common complaint in such environments, leading SOC professionals to ignore alerts, pay to hire more staff to share the burden, or even leave their post entirely.⁷



By reducing the number of repetitive tasks performed by personnel and automating common security processes, organisations can bolster morale, build a more strategic SOC, and more easily take a multilayered approach to security with fewer resources.

⁷ CRITICALSTART. (2019). The Impact of Security Alert Overload.

CHAPTER 5

Effective tools and skilled resources

There is only so much an organisation can do without the right tools, technologies, and resources. The operative word being “right.” A Ponemon Institute report found that companies have an average of 47 different cybersecurity solutions and technologies deployed.⁸ The same report notes that more than half (53%) of IT experts don’t know how well the cybersecurity tools they’ve deployed are working, and only 39% say they are getting full value from their security investments.

What is the issue? There are several:



Having the time or expertise to make sound decisions regarding security products or platforms



Understanding the skill sets required to deploy, adopt, integrate, customise, and optimise security investments



Complex IT environments (due to rapid growth, M&A activity, etc.) with innumerable vectors of attack



Aligning IT investments with budgets, which sometimes results in unfortunate compromises



Acquiring point solutions that each offer limited scope and contribute to tool fatigue



Finding and retaining key security talent

IT directors need to continuously re-evaluate their risk posture and threat response capabilities, while taking advantage of the latest security offerings. By aligning closely with business and line-of-business leaders, IT organisations can also ensure the buy-in needed to develop a security-savvy organisation and minimise the occurrence of shadow IT and other risky behaviors.

How do you address these concerns and drive meaningful improvements in your security operations?



⁸ Ponemon Institute. (2019). The Cybersecurity Illusion: The Emperor Has No Clothes. Sponsored by AttackIQ.

Look to trusted sources

Insight helps companies like yours assess their security environment, develop an actionable roadmap, implement the optimal solutions, and manage a best-in-class SOC that boasts all five attributes described here. Our premise is that security is not purely a technology issue but a business priority — we combine technical and consulting experience and intelligence to augment your entire security program.

One way we deliver is with Microsoft® Sentinel™, a cloud-native Security Information and Event Management (SIEM) and Security Orchestration and Automated Response (SOAR) solution that collects security data across the entire hybrid enterprise and uses the power of Artificial Intelligence (AI) to rapidly identify and investigate threats.

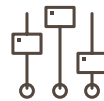
Why Insight and Microsoft Sentinel?



Maximise the benefits and capabilities of your security investments



Better align security efforts with business objectives



Improve the security, visibility, and control of your entire IT environment



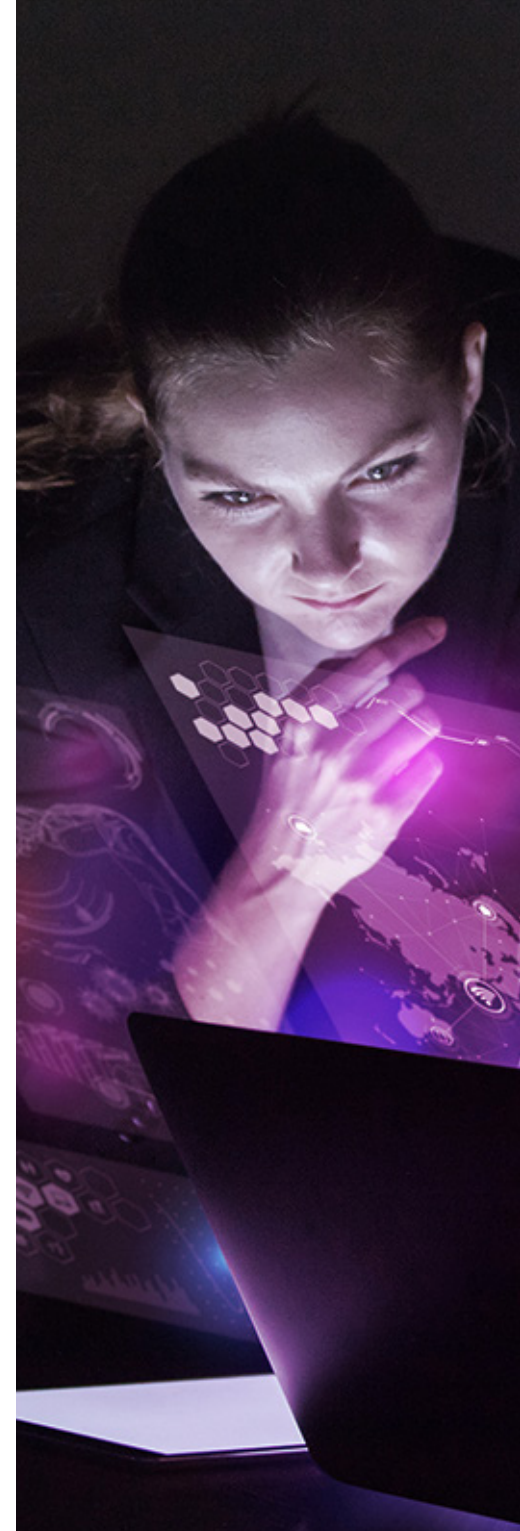
Accelerate and automate the hunting and detection of cyberthreats



Offload the task of monitoring your network, systems, applications, and data



Reduce risks and make security-related costs more predictable



About Insight



More than 20 years of support services delivery



PCI DSS compliant, SOC 2 Type II certified, ISO 27000 certified, and a member of TSANet and TSIA



A leading Microsoft partner with
18 Gold & Silver competencies



**Azure
Expert
MSP**

An Azure Expert Managed Services
Provider (MSP) and the **largest
Azure partner**



**Recently named a Microsoft Security
20/20 award winner** for the Azure Security
Deployment Partner of the Year category

What does Microsoft say?

Ann Johnson, corporate vice president of Cybersecurity Solutions at Microsoft, said, "By combining our Microsoft security portfolio with Insight's security services, we empower our customers to modernise their security operations. Cybersecurity is complex, but it doesn't have to be complicated. Advancing our security relationship with Insight helps organisations simplify their security operations and scale as they grow."



About Microsoft Sentinel

- Quick and relatively easy to deploy, greenfield or via log redirection
- Flexible and scalable, allowing for dynamic adjustments for workloads or compliance
- Cost-effective, with no upfront costs or hardware requirements
- Developed and consistently enhanced by IT and security industry leaders
- Leverages the latest, cutting-edge AI and machine learning capabilities



Gain the tools and expertise you need to hit all five attributes described in this ebook. Get started with Insight and Microsoft Sentinel today.

Contact us

uk.insight.com