Virtually extend your security team and quickly add expertise

—

John Wheeler
BISO, IBM Security
VP of Strategy and Innovation, Services and Integrated Solutions

Melissa Thomann
Director, Client Services – Global Managed Security Services
Organizations are forced to rapidly evolve

- **Speed of change**
  - Digital transformation

- **Complexity**
  - Hybrid multicloud

- **Accountability**
  - Beyond responsibilities

- **Expertise**
  - New competency and specialized skills

Evolving Global, Business and Threat Landscape

Compliance, Privacy, and Regulatory Requirements
Remote work is a culture change for most companies and employees

- Newly connected devices on network
- Teams impacted
- Resources may not be available
- Cost optimization may be a factor
Six Best Practices

Help secure remote access

1. Secure computers and devices
   - AV software, host-based firewall, or EDR solution
   - Monitor regularly and encrypt data at rest

2. Review home-based security
   - Update routers, printers, and any connected device
   - Keep work computer isolated from personal

3. Public internet access
   - Always use 2FA along with VPN connectivity
   - Never connect to an unsecured network

4. Public cloud or storage devices
   - Only use corporate owned storage devices
   - Ensure data transfer is done over VPN

5. Phishing attempts
   - Double check links from email and be suspicious of emails
   - Ensure devices are setup with Mobile Device Management (MDM)

6. Encrypted communications
   - Use official and secure communication channels
   - Use a virtual desktop when an official machine is not used
Here’s what we see from clients across various security environments
314
Average number of days in a lifecycle of a malicious attack breach

279
Average number of days to identify and contain a breach
Average number of vulnerabilities reported by scanners in client environments

1.7M
How are phishing threat actors capitalizing on COVID-19?

Spoofing of WHO, CDC and other official health organizations
Your first line of defense
Train and educate your user base

- Reduce number of incidents and exposure to cyber threats by strengthening employee awareness
- Minimize overall cost of incidents
- Consistent awareness program implementation across organization
- Conduct live phishing tests with targeted training
- Increase security awareness and behavioral change
68% of organizations were victims of endpoint attacks in 2019.

Source: 2020 Ponemon Institute State of Endpoint Security
Effective endpoint defense begins with 24x7 detection, threat hunting, and response built on intel

Rapid response and active blocking
Automate threat mitigation and extend your team with threat experts to help you respond and proactively block threats

Deep visibility and investigations
Global world-class threat intelligence combined with endpoint visibility to protect you from advanced threats 24x7

Complete security without complexity
Support for detection, response, and threat hunting for multiple EDR/next generation anti-virus vendors in the same environment

Consistent outcomes for threat protection
Focus on tactics, techniques and procedures, to find threats more consistently than static Indicators of Compromise (IOCs)
Global healthcare provider

Securely scales to provide telemedicine services and adapts to remote workforce.

During a major infrastructure migration and upgrade, the business simultaneously adapted to the changing global landscape and pandemic.

Business problem

- Delay in cutting over to the new infrastructure would have resulted in significant increase in the TCO
- Scale up and provide a safe remote working environment to the user base who traditionally never worked from home
- Set up a secure telemedicine infrastructure

Solution

- Adapted to inflight changes during the migration and upgrade
- Designed and implemented an entirely new remote working infrastructure
- Assisted users adapting to the rapidly changing work environment
- Designed, tested and implemented additional use cases in the SOC to respond to changes
- Prepared for the new reality
Client had a previous configuration to allow VPN connectivity, however the Global Protect feature required additional tuning in support of having significantly more users connecting remotely.

Business problem

- Complex configuration required to match level of authorization based on users’ profile
- Configuration changes needed to allow privilege level enforcing
- Large global network with users in 60+ different sites around the globe

Solution

- IBM MSS aided in consulting over multiple sessions to extend client’s remote support capabilities
- Configuration of client’s network was extended through different sites using interconnectivity between Palo Alto firewalls in each location and the Panorama management platform.
- IBM MSS assisted the Client with extending their VPN access capabilities to a minimum of 200 concurrent users per site, or 1000 users connected using global protect software
## Choosing the right security partner

### Faster, more relevant detection and response
- AI/ML + human expertise applied to reduce false alerts, eliminate fatigue, and rapidly respond
- 100+ investigation experts to assist with on-the-ground response

### Trusted security advisors
- Dedicated security experts with strong vertical expertise
- Personalized advisory services integrated into your MSS
- Holistic approach to secure hybrid cloud environments

### Global scale, local delivery
- Hybrid delivery models to meet clients anywhere in the world
- Staff on the ground for local, personalized delivery

### Demonstrate security impact and value
- Measured security effectiveness
- Regular security posture reporting
- Industry comparison reports

### Translate risk into action
- Actionable context through a single, integrate GRC platform
- Detailed GRC visibility with powerful dashboards
- Classify and categorize events, risks, issues to improve data quality and improve compliance efficiency
IBM Security has invested millions preparing for moments like this one.

We have demonstrated our resilience in the face of fires, floods, earthquakes, tsunamis, blackouts, lighting strikes, blizzards, and more.

Our robust set of business continuity plans and globally distributed operations, which pandemic planning, mean we can execute for our clients with calm and confidence.

Learn more at: https://www.ibm.com/security/COVID-19
Resources

IBM Security X-Force Threat Management Services
https://www.ibm.com/security/services/threat-management

IBM Managed Security Services
https://www.ibm.com/security/services/managed-security-services

IBM Security X-Force Red
https://www.ibm.com/security/services/offensive-security-services

IBM X-Force Incident Response and Intelligence Services
Thank you

**John Wheeler**  
BISO, IBM Security  
VP of Strategy and Innovation, Services and Integrated Solutions

**Melissa Thomann**  
Director, Client Services – Global Managed Security Services
Notices and disclaimers

© 2020 International Business Machines Corporation. No part of this document may be reproduced or transmitted in any form without written permission from IBM.

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. This document is distributed “as is” without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity. IBM products and services are warranted per the terms and conditions of the agreements under which they are provided. The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply.”

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.
Notices and disclaimers continued

It is the customer’s responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer’s business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM’s products. IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at:
Please note

IBM’s statements regarding its plans, directions, and intent are subject to change or withdrawal without notice and at IBM’s sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user’s job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.