The Changing Face of Cybersecurity

Johna Till Johnson, CEO & Founder
Nemertes Research
July 17, 2019
The Cybersecurity Seismic Shift
The “Good Old Days”: Better Bad Guys...

- External actors
- Simpler motives
- Fewer threat vectors
- Human, not AI
- Employees, customers, suppliers could be presumed to be safe (with rare exceptions)
The “Good Old Days”: Safer Spaces...

• Critical data, systems on-prem
• Firewalls kept bad guys (and apps) out
• Fewer devices, systems, users, apps
The “Good Old Days”: Slower Pace!
The New World Order: Five Foundational Shifts

- Shift #1: From deliberate to agile
- Shift #2: From perimeter-based to zero-trust
- Shift #3: From on-prem to cloud
- Shift #4: From manual to intelligent automation
- Shift #5: From appliances to software
The New World Order: Five Foundational Shifts

- Shift #1: From deliberate to agile
The New World Order: Five Foundational Shifts

• Shift #1: From deliberate to agile
• Shift #2: From perimeter-based to zero-trust
The New World Order: Five Foundational Shifts

• Shift #1: From deliberate to agile
• Shift #2: From perimeter-based to zero-trust
• Shift #3: From on-prem to cloud
The New World Order: Five Foundational Shifts

- Shift #1: From deliberate to agile
- Shift #2: From perimeter-based to zero-trust
- Shift #3: From on-prem to cloud
- Shift #4: From manual to intelligent automation
The New World Order: Five Foundational Shifts

- Shift #1: From deliberate to agile
- Shift #2: From perimeter-based to zero-trust
- Shift #3: From on-prem to cloud
- Shift #4: From manual to intelligent automation
- Shift #5: From appliances to software
SHIFT #1: AGILITY
Unprepared (Level 0)

- Lacking necessary information to take effective action; unaware or unable to respond to current or emerging issues

Reactive (Level 1)

- Have basic platforms and structures to react to business requirements; cannot proactively prevent problems from arising

Proactive (Level 2)

- Have platforms, structures, organizational processes to proactively address current issues and challenges

Anticipatory (Level 3)

- Have platforms, structures, organizational processes to proactively address future issues and challenges
Incident Containment Time

Detect  Understand  Contain

Total Time to Contain (TTC)
Cybersecurity TTC 2018

98th percentile

8 minutes

75th percentile

109 minutes

50th percentile

410 minutes

Anticipatory

Proactive

Reactive

© 2019 Nemertes Research   DN7777
Cybersecurity TTC 2019

- **Anticipatory**
  - 98th percentile
  - 2 minutes

- **Proactive**
  - 80th percentile
  - 20 minutes

- **Reactive**
  - 50th percentile
  - 180 minutes

© 2019 Nemertes Research   DN7777
Cybersecurity Success Group 2019

- **Anticipatory**
  - 98th percentile
  - "Success Group" = 80th percentile; those with TTC of <20 minutes

- **Proactive**
  - 80th percentile

- **Reactive**
  - 50th percentile

© 2019 Nemertes Research   DN7777
Definitions:

- **Incident** = confirmed attempted breach or attack
- **Serious** incident has an impact on employees, businesses, or customers (or all three) or necessitates contact with external authorities
SHIFT #2: ZERO-TRUST
Zero-Trust On the Rise

State of Adoption: Zero Trust

- Using Now: 34%
- Planning for 2019: 18%
- Planning for 2020: 17%
- Evaluating: 15%
- Evaluated and Rejected: 3%
- No Plans: 9%
- Don't Know: 4%

State of Adoption:

- Financial Firms: 36% using now
- Success Group: 33% using now
Zero Trust Comes of Age

When Did You Launch Zero Trust?

- In 2018: 62%
- In 2017: 13%
- In 2015 or previously: 13%
- In 2019: 12%

When Did You Launch Zero Trust?
The zero-trust approach to security is an emerging paradigm that supersedes the perimeter-based model. With perimeter-based security, resources and users on the inside of the perimeter are assumed to be trusted, while those that are external are untrusted.

With zero-trust security, in contrast, trust is highly granular and distributed. One microservice running on a cloud platform may be trusted, while another microservice running beside it on the same platform may not be.

Zero-trust depends on having highly granular (and accurate) data classification as well as deep segmentation of network and compute resources.
Zero-Trust Security Roadmap

Deploy foundational technologies
- Deep segmentation
- Microservices
- Next-generation endpoint protection
- Container security
- Behavioral threat analytics (BTA)
- CASB
- Cloud DLP and IAM
- IoT security

Develop trust models and processes
- Devices
- Locations (remote site, cloud, IoT)
- Applications
- Services
- Microservices
- Containers
- Data
- Users (employees, customers, third-parties)

Automate and integrate
- Configuration/updates
- Response management
- Threat intelligence
- Third parties (risk assessment, supply chain)
SHIFT #3: CLOUD
2019: Year of CASB

State of Adoption: CASB

- Using Now: 44%
- Planning for 2019: 22%
- Planning for 2020: 10%
- Evaluating: 12%
- Evaluated and Rejected: 1%
- No Plans: 8%
- Don't Know: 3%
- State of Adoption: CASB

Financial Firms:
- 36% using now

Success Group:
- 52% using now
Cloud access security brokers (CASBs) provide additional security controls on and visibility into enterprise use of cloud resources. They can be in-line proxy-style intermediaries through which cloud-bound traffic passes, or they can be API-based services that are called upon by cloud services for authentication and authorization of user access, and to which cloud services send monitoring event information on use of the service. Examples include:

- BitGlass
- Blue Coat/Symantec
- Microsoft
- Skyhigh
- Netskope
Implement
- Select and deploy with cloud and applications
- Validate dashboard, performance, and metrics
- Confirm response processes (both human and automated) for anomalies, alerts, and incidents

Integrate
- Integrate as appropriate with adjacent technologies (BTA, ESCAPE, mobile devices, MFA, threat intelligence, CloudSSO and IAM)
- Leverage APIs as needed

Enhance
- Enable missing capabilities (depending on solution) including enhanced analytics, proactive management, etc.
Enterprise Secure Cloud Access and Policy Enforcement (ESCAPE)

Mobile and home users and even sites connect via secure PoP

Policy applied, CASB style: in-line or by API

Access granted or blocked to private resources or public SaaS or IaaS

Cisco Umbrella, Palo Alto Prism, Cato, others

Branch on WAN
Branch on Internet
IoT

AWS
GCP...
Azure

Office 360
Google Suite
Salesforce
Etc...

DC

© 2019 Nemertes Research  DN7777
ESCAPE Gaining Traction

State of Adoption: ESCAPE

- Using Now: 38%
- Planning for 2019: 24%
- Planning for 2020: 8%
- Evaluating: 15%
- Evaluated and Rejected: 1%
- No Plans: 12%
- Don’t Know: 2%

Financial Firms: 36% using now
Success Group: 52% using now

© 2019 Nemertes Research  DN7777
ESCAPE platforms provide a centralized platform from which enterprises can manage, secure access to, and enforce policies across distributed multicloud resources and devices.

Examples include:

- Cisco Umbrella
- Palo Alto Prisma (formerly Global Protect Cloud Service)
- Symantec Integrated Cyber Defense
ESCAPE Roadmap

Find initial use case and options
- Mobile users, or small branches?
- Find best PoC subset within chosen case
- Demonstrate secure access, CASB, SSO capabilities
- Develop baseline policies in line with evolving ZT
- Select solution

Expand Use
- Expand within chosen use case, beyond PoC
- Select PoC group(s) for other use case
- Extend to compliance management and audit
- Fully integrate with cloud config automation, infrastructure as code, etc.

Complete Deployment
- Wrap up remaining groups of users and locations

Evaluate Options
- Consider migration or supplementation for special use cases
- Require ability to unify policy

2019 2020 2021 2022
SHIFT #4: INTELLIGENT AUTOMATION
BTA Takes Center Stage

State of Adoption: BTA

- **Using Now: 31%**
- **Planning for 2019: 26%**
- **Planning for 2020: 11%**
- **Evaluating: 16%**
- **Evaluated and Rejected: 2%**
- **No Plans: 12%**
- **Don't Know: 2%**

**State of Adoption: Financial Firms**

- **36% using now**

**State of Adoption: Success Group**

- **48% using now**
BTA Cliffs Notes

BTA (also referred to as user and entity behavioral analytics, UEBA) is software that integrates multiple sources of data (logs, analytics platforms, SEIM) to capture and display anomalous behavior of users, devices, and systems. BTA solutions can rely on a mix of AI, ML, rules engines, and big data.

Examples include:

• Bay Dynamics
• Gurucul
• Exabeam
• Splunk/Caspida
Deploy and integrate foundational technologies

- SIEM if needed
- IDS/IPS
- Firewalls if selected
- Data logs
- IoT data (human/facilities)
- Cloud/CASB data

Enhance processes

- Select processes for automation
- Strengthen IRP (especially for cloud)
- Fine-tune dashboards, metrics, and reports
- Impose any needed Digital Ethics controls
- Develop information stewardship strategy

Enhance automation

- Automate selected incident responses
- Optimize performance (increase percentage of incidents handled automatically)
- Integrate into additional systems

2019 | 2020 | 2021 | 2022
SHIFT #5: SOFTWARE
Containers Are Key...

State of Adoption: Containers

- Using Now: 35%
- Planning for 2019: 25%
- Planning for 2020: 13%
- Evaluating: 14%
- Evaluated and Rejected: 1%
- No Plans: 9%
- Don't Know: 3%

Financial Firms
- 36% using now

Success Group
- 48% using now
...So is Securing Them!

State of Adoption: Container Security

- Using Now: 73%
- Planning for 2019: 18%
- Evaluating: 9%

Note: Only selected users of containers participated in the drilldown on containers. Thus, this represents a portion of the 35% in the previous chart.

Container security is software specifically for adding security layers to a container environment by enabling technologists to set and enforce policies for containers (eg Docker) and container orchestrators (eg Kubernetes). Vendors include:

- Aqua Security
- Capsule8
- LayeredInsight
- NeuVector
- StackRox
- Tenable
- Tigra
- Twistlock (now Palo Alto)
TAKEAWAYS
Actionable Takeaways

1. Assess framework, architecture, and roadmap against five shifts. Are you ready?

2. Perform gap analysis of existing technology solutions. What capabilities are you missing?

3. Reassess cybersecurity team, organization structure, operations in light of revised strategy. What needs to change?

4. Focus efforts on improving TTC; this will drive an emphasis on analytics and automation.

5. Drink more coffee. You’ll need it!
METHODOLOGY AND DEMOGRAPHICS
Developed hypotheses in consultation with clients and others (Jan-March 2019)

Conducted benchmark interviews and online surveys (March-June 2019)

Analyzed findings to validate hypotheses (July 2019)
<table>
<thead>
<tr>
<th>Statistic</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participating Firms</td>
<td>335</td>
</tr>
<tr>
<td>Countries</td>
<td>11</td>
</tr>
<tr>
<td>Vertical industries</td>
<td>24</td>
</tr>
<tr>
<td>Mean employee count</td>
<td>8890</td>
</tr>
<tr>
<td>Median employee count</td>
<td>1650</td>
</tr>
<tr>
<td>Mean annual revenue</td>
<td>$2.3 B</td>
</tr>
<tr>
<td>Median annual revenue</td>
<td>$125 M</td>
</tr>
</tbody>
</table>
Thank you!

client-services@nemertes.com
sales@nemertes.com
@Nemertes