Research Note: RSA Conference 2019

Rajeev Chand
Partner
Head of Research

Wing Venture Capital
2061 Avy Avenue
Menlo Park, CA 94063

The 28th annual RSA Conference was held March 4-8, 2019, at the Moscone Center in San Francisco, California. The conference is one of the largest conferences for information security globally and hosted 42,500+ attendees.

At this year's RSA, we held 21 1-on-1 meetings with CISOs/CSOs, entrepreneurs, and government officials over two days, and we hosted the inaugural Wing Summit on Security, involving 101 CISOs/CSOs from large cap public companies and 'unicorn' private tech companies in an off-the-record, closed-door setting. In addition, we held 26 pre-RSA research calls with CISOs/CSOs and government officials to understand key security issues and priorities.

In this Research Note, we highlight the trends, insights, and observations from our conversations in the following sections:

- Key News Announcements
- CISO Priorities
- Government and Private Sector

Key News Announcements

There were two news announcements that were prominent in our RSA 2019 meetings: 1) Chronicle's launch of Backstory, and 2) NSA's release Ghidra.

Backstory

Chronicle's launch of Backstory was the most discussed item in our meetings. We had two observations:

1) There is pent-up demand for a Splunk alternative. Splunk has the advantage of incumbency, and Splunk is 'more than an application, it is a way of doing business', as stated by a colleague. However, Splunk's data-based pricing model was frequently mentioned as expensive. A colleague commented, 'each year we re-examine whether this is the year to replace Splunk, and each year Splunk reduces its price sufficiently to make the transition costs for tools and processes not worth it.'

2) The most often mentioned critiques of Backstory were: a) would corporations trust Google with their telemetry data, and b) does Backstory have the product maturity required by large enterprises.

- On trust, our conversations were mixed. Executives acknowledged a concern, but some felt the concern was a non-issue.

- On maturity, some expressed concerns on features and capabilities. One executive commented, ‘Backstory will find a place, but it is Splunk six years ago.’ Another commented, ‘it is massively over-hyped.’

Overall, we found that Backstory had broad interest and early momentum, despite the reservations discussed above.

Ghidra

NSA’s release of Ghidra malware reengineering tool was one of the exciting developments at RSA. One executive commented that his engineers were ‘playing with it until 3 a.m.’ and thought highly of the tool.

Additional Announcements

A summary of additional announcements at RSA 2019 is included in the Appendix of this Research Note.

CISO Priorities

In our meetings and calls with CISOs/CSOs, we focused on the questions: 1) what is the state of security, and 2) what is the most important challenge that you are facing?

State of Security

We found a state of security that is ‘short-term pessimistic and long-term optimistic,’ as stated by a colleague. At RSA 2018, Cisco’s keynote stated, ‘we are completely screwed, even more than we were last year.’ In our view, little (or not enough) has changed to shift the state of security over the past year. One CSO commented this year, ‘security is like an expanding rubber band where the bad guys are pulling on one side at an increasing rate while many corporations on the other side are still treating security as an add-on to IT.’ With that said, we also found optimism. One colleague commented, ‘digital business is still occurring and is growing rapidly.’ Further, as discussed below, security is now a board- and Davos-level topic.

Supply Chain

Supply chain security (third-party, fourth-party) was the most frequently discussed new topic in our meetings—and was raised by both chief product security and chief information security officers. In our view, supply chain security has significantly more unanswered questions than it has practical solutions. We had three observations:

1) The current approaches of questionnaire-based self-assessments have inherent limitations. One vendor commented, ‘we do not know how others fill out the forms, and we find gradations in possible responses.’

2) The levels of interdependence, globalization, and fragmentation among corporations are remarkably high and increasing, yet the levels of visibility and control are low to none, as commented to us by a CSO.

3) The solutions discussed in our meetings varied widely. Comments included:

- 'We are placing governance requirements on our suppliers, such as a CSO position, and we are mapping our suppliers' suppliers to assess fourth-party concentration.'
- 'We are not investing to try to understand more. Our approach is focused on improving resilience.'
- 'The more nuclear you can get about trust, the better.'

Board Involvement

One major change over the past year is the increased involvement in boards in security. A colleague commented, 'the board is now an interested and active party in security,' and another commented, 'most boards now have at least one member who has gone through a major breach' since independent members sit on multiple boards. The trend, however, is early. A colleague commented, 'progressive boards that are active in cybersecurity are still in the minority.' A CSO questioned, 'do we need an Enron for security' to truly raise board involvement further.

We had two observations:

1) There is a wide range of board engagement, at times based on the interest and composition of the board, and best practices are not clear. For example, one CISO in our meetings spends 20 minutes presenting to the board, while another spends half-a-day presenting and discussing.

2) There is a next evolution of the board discussion—to drive to business metrics, quantify risk scenarios, and make proactive risk management decisions. A colleague commented, 'security discussions today are like accounting prior to GAAP.' In our view, most board members leave security updates dissatisfied and unsure of whether security is really under control or what to do.

Basics & Cyber Hygiene

A focus on the basics was a recurring theme in our conversations with CISOs and CSOs. One executive commented, '80% of the problem can be solved by getting the cyber hygiene correct, rather than chasing the latest advanced technology.' Another remarked that 'security is now a topic at Davos,' where the imperative is to 'get the world of small-to-mid sized enterprises and large enterprises to pay attention to the basics.'

Interestingly, another CSO commented, 'we need to continuously monitor even the things that we have fixed; everyone has discovered items that they thought were fixed but were no longer fixed.' Cyber hygiene, although not distinctive or remarkable, is a major opportunity in security.

'31 Flavors' of Vendor Fragmentation

Vendor fragmentation is a significant issue in security. As an example, the market landscape slide in Momentum Cyber's annual report is one of the densest maps of startups that we have seen in our experience. Anecdotally, we hear that corporations have ~25-30 security vendors. Cisco reports that large corporations have up to 70 security vendors. One CSO commented, 'I do not need the 31 flavors of the latest security solutions.' Numerous colleagues indicated a desire or a strategy to consolidate and rationalize security vendors.

Machine Learning

Machine learning is at a nascent stage in security. The opportunity is significant, as the data sets available for security processing are unprecedented in size, complexity, and growth. As one executive quipped, 'at no time at RSA did I hear a person say I want to get more alerts.'

Most executives in our meetings were skeptical on ML solutions from security vendors. One commented, 'the big issue today is that the suppliers are all stating ML but are selling to executives who do not necessarily understand ML.' Another commented, 'most advertised AI is really ML, and most ML is really fancy correlation.'

Some CISOs/CSOs in our meetings had successful examples of ML, while many did not. One CISO commented, 'I have been able to use ML in specific and limited use cases, but it is not the holy grail and it is expensive.' One CSO commented, 'no one relies on ML the way that we had expected.'

We also found two interesting uncertainties in our research conversations. First, the policies and procedures for processing unanticipated results from ML are not clear. One CISO commented, 'we are cross-pollinating data that had been previously siloed and are generating unanticipated results and insights that our analysts and investigators are not necessarily accustomed to.' Second, the balance between embracing ML and maintaining data security is not clear. One CSO commented, 'CEOs and CTOs are telling us to embrace data science environments that require large samples or full sets of data, yet we do not really know what the data scientists will do with our data.'

CISO Organizational Structure

In our view, organizations continue to struggle with where the security function should report, how it should be led, and how it should be organized. The reporting relationships for CISOs/CSOs was a topic of strong interest in our meetings. Although all acknowledged that 'it depends' is the broad answer, the approaches varied dramatically. Comments included:

- 'CSOs should not report to the CEO; they should be a layer removed and have a direct connection to the audit & risk committee.'

- ‘Security needs to be separated. Security engineering can be distributed and embedded, while security governance and compliance can be centralized.’
- ‘CSOs should report to the CEO.’

Although each organization is different, in our view, the most important dynamic is the trust and access between the CISO and the CEO/board, irrespective of the reporting relationship or organization structure.

Interestingly, another CSO commented on the role for CSOs as independent board members. He said, ‘CSOs should be independent board members on large corporations, just like there are independent positions for digital or tech.’

CISO Profession

The profession and the life of a CISO was another frequently discussed topic in our meetings. Numerous colleagues mentioned the recent study that 1 in 6 security leaders have alcohol or substance abuse issues. The average tenure for a CISO is approximately 18-24 months. One CSO quipped, ‘CSO stands for Chief Sacrificial lamb Officer.’ Another quipped, ‘it is normal to feel like you have a micro-version of PTSD.’ The CISO profession is a demanding, stressful role.

In addition, we had several interesting conversations on the seniority level and the career path for CISOs.

- On seniority level, several colleagues questioned what the appropriate title level – EVP, SVP, VP – and the associated compensation level should be for a CISO.
- On the career path, one CISO questioned, ‘where do we go after being CISO.’ Interestingly, one director-level colleague said, ‘I told my CTO that I do not want to be in CISO team; I want to be in engineering team where I have a long-term path.’ Another CSO emphasized, ‘there is a next level of the CISO role that we need to get to; we can be the business partner for every discussion by the CEO and the management team on trust and privacy.’

Additional Topics

Other topics in our meetings included: IoT, which one colleague dubbed the ‘Internet of Threats’; privacy, especially with GDPR and CCPA; trust, especially as it relates to brand recovery; blockchain; automated pen testing; zero trust technology; edge security; IT and OT; cloud security; product liability for security; and DevSecOps.

Government and Private Sector

The threat to corporations from nation-state and nation-state financed attacks is more significant in the current landscape. Crowdstrike, McAfee, and Symantec recently issued reports discovering increased activity by China, North Korea, Russia, and Iran. Some colleagues in our meetings questioned the ‘marketing’ value of the reports; however, the trend is clear.

We focused our discussions on government/private sector relations on two topics: 1) information sharing, and 2) role of military in nation-state attacks on corporations.

Information Sharing

We heard resounding concerns in our meetings with CISOs/CSOs on information sharing with the U.S. government. Comments included:

- 'It is [expletive] useless.'
- 'DHS is happy when they give us information 9 months after it occurred.'
- 'Threat intel is still unilateral. When I ask for information, I get nothing, and when they come asking, I do not necessarily feel inclined to help.'
- 'I understand that government has broader national security goals, but I do not want to be the collateral damage.'
- 'We get more details in the New York Times.'

Although government colleagues in our conversations agreed that information is over-classified, they cautioned on several key points. 1) One colleague commented, 'there are misperceptions on both sides; the private sector believes that if they knew what we know that they would be safe.' 2) Another colleague commented, 'the government does not have the resources to take on a mandate to protect everyone and everything.' 3) Another colleague commented, 'we do not want to create a too-big-to-fail like scenario where the private sector is disincented to invest in their protection.'

Interestingly, a CSO also argued, 'the information that corporate CSOs want is available, and we need to build the capabilities to find it.'

In our view, although information sharing is an area with the need for dramatic change, we do not see a near-term driver to materially improve the current dynamic.

Military Role in Nation-State Attacks on Corporations

We also found a debate on the role of the U.S. military in nation-state attacks on U.S. corporations. Currently, U.S. Cyber Command does not have the authorities to respond on behalf of corporations, and it is an open question as to whether they will gain those authorities.

The proponents for a role argued that: 1) there is an imbalance in resources and capabilities between nation-states and corporations, and 2) the U.S. military has a role in potential kinetic attacks against U.S. corporations—which not be that dissimilar to that in potential cyber attacks.

In our conversations, numerous CISOs/CSOs were cautious on military involvement. Selected concerns included: 1) will military involvement inadvertently escalate the situation and drive unintended, derivative, and broader attacks; 2) will the military's objectives (e.g. observation) conflict and precede the corporation's objectives (e.g. remediation and resilience); and 3) will intelligence be able to be certain enough to know the actual attacker.

Additional Topics

Other topics in our meetings included: government backdoors and encryption; critical infrastructure; U.S. elections; vendor national security risks and reciprocation; state of cyberwar ‘unpeace;’ and forced technology transfers.

Conclusion

Overall, we left RSA with the sentiment that security is not solved – and is inadequate and broken in many cases – but it is “Better”, which was the theme of RSA 2019. For entrepreneurs, a significant challenge is to rise above the noise and establish a dramatically different value proposition to offset the CISO/CSO concerns on vendor fragmentation and fatigue. For CISOs/CSOs, a new challenge is to leverage the opportunities for board engagement in security to drive to business metrics and decisions around risk, trust, and privacy. The ongoing change and opportunity in security has never been greater.

Wing Venture Capital is an early stage venture capital firm focused on seed and series A investments in business technology. As disclosure, a list of Wing’s portfolio companies is available on Wing’s website at wing.vc/companies.

We would like to thank Brendan Baker for his research and contribution to this Research Note.

Appendix – RSA 2019 Selected Announcements

Application Security

- **Synopsys:** introduced Polaris Software Integrity Platform, a cloud-based platform for comprehensive application security from development to deployment.
- **Virsec:** launched Application Memory Firewall, an advanced memory protection solution to detect and take action on deviations in application execution caused by memory-based attacks.
- **Wallarm:** launched Cybersecurity Transparency Initiative to enable continuous security through collaboration, transparency, and automation.

Blockchain

- **IBM:** launched X-Force Red cybersecurity service for enterprise blockchain for stress and penetration testing.

Cloud Security

- **APCON:** announced availability of IntellaCloud for AWS network visibility for NetOps and SecOps teams.
- **CyberArk:** published research on container escape routes demonstrating that certain Linux security controls where the host kernel is vulnerable can be further manipulated to allow attackers to escape.
- **FireMon:** announced Lumeta CloudVisibility for cloud visibility, security, and anomaly detection for hybrid enterprises.
- **Forcepoint:** announced the Forcepoint Converged Security Platform for secure migration of data, applications, and business operations to the cloud.
- **Fortanix:** launched an Enclave Development Platform based on an open source SDK written in Rust and optimized for Intel Software Guard Extensions.
- **Infoblox:** announced Network Identity Operating System 8.4 platform, including support for Google Cloud Platform and single sign-on.
- **Marvell:** announced LiquidSecurity Network HSM for enterprise data center and private cloud markets.
- **Sysdig:** announced new features for its Cloud-Native Intelligence Platform that extend compliance metrics and Kubernetes audit events to a monitoring dashboard and that make compliance data available by default.
- **Twistlock:** announced the release of Twistlock 19.03 with cloud native security protection of hosts, containers, and serverless.

Cyber Insurance

- **Cytegic:** announced partnership with The Phoenix Insurance Company for cyber insurance for small and medium-sized enterprises.

Data Security

- **BigID:** unveiled new data access intelligence capabilities to BigID's Data Intelligence Platform to pinpoint systems and employees with access to personal information.

- **Cryptshare:** launched Cryptshare.express, a SaaS-based solution for SMBs for secure transmission of large, encrypted files or email messages.
- **Cryptshare:** announced release of Cryptshare QUICK Technology, a security solution for encrypted data transmission, in Europe immediately and in U.S. in early April.
- **MyWorkDrive:** introduced new features in MyWorkDrive Version 5.2, including SAML Login, simplified directory integrations, administrative alerts, and DLP enhancements.
- **nCipher:** announced enhanced remote access to the crypto capabilities in its nShield Connect XC HSMs.
- **NSA:** released Ghidra, a free software reverse engineering tool that had been an internal tool within the NSA and that can analyze binaries written for a wide variety of architectures.
- **SecureCircle:** announced the availability of SecureCircle version 2.5, which includes agentless secure collaboration via Send Secure.
- **Teramind:** announced the availability of its privacy-friendly software solutions for insider threat detection and DLP compliance with privacy requirements such as GDPR and CCPA.

Endpoint Security

- **Adaptiva:** introduced Evolve VM, which detects and remediates compliance issues and vulnerabilities across endpoints through P2P technology.
- **AttackIQ:** announced partnership with Blackberry Cylance to validate endpoint security solution deployment and configuration.
- **Blackberry Cylance:** introduced CylancePERSONA, a proactive endpoint behavioral analytics solution.
- **Digita:** demonstrated GamePlan, a suspicious activity detection tool for Macs that uses Apple's GameplayKit framework.
- **Eclypsium:** announced partnership with Intel to help organizations manage firmware attacks.
- **Intel:** unveiled Threat Detection Technology, silicon-level capabilities that shift memory-based attack monitoring from the CPU to an integrated GPU and that use machine learning algorithms to search telemetry for advanced threats.
- **NSS Labs:** Released 2019 Advanced Endpoint Protection Group Test, recommending 14 of 19 products and noting an improvement in security effectiveness year over year.
- **SentinelOne:** announced the integration of Intel's Threat Detection Technology Accelerated Memory Scanning capabilities with the SentinelOne's autonomous endpoint protection console.
- **SentinelOne:** released Full Remote Shell capabilities to allow authorized administrators to access managed endpoints and establish a full remote shell session from the SentinelOne console UI.
- **SentinelOne:** announced ActiveEDR, an endpoint security solution to understand the root cause behind threat actors and autonomously respond without reliance on cloud resources.
- **SparkCognition:** released DeepArmor version 2.0 with new capabilities including agent support for Linux OS, machine learning detection engine for malware attacks, expansion of telemetry, and autonomous alert handling.

Identity and Access Management

- **Armor Scientific:** announced the Armor Platform, a converged, wearable GPS hardware token and middleware suite for identity management.
- **BioCatch:** announced receipt of U.S. patent covering methods of assessing the level of pressure that a user applies to a given touchscreen or other electronic system.

- **BioConnect and ForgeRock:** announced partnership to enables companies to secure privileged access with enterprise grade, multi modal-biometrics.
- **CyberArk:** announced new capabilities for CyberArk Privileged Access Security Solution v10.8 for detection automation and user access flexibility.
- **FEITAN:** launched Fingerprint Power Card that combines multiple security technologies in one card, including authentication, physical access, identification, payment, and access to applications or data.
- **ImageWare Systems:** announced the ImageWare Digital Identity Platform, an integrated suite of products that provides biometric authentication factors and identity proofing capabilities.
- **Pulse:** announced integration of Software Defined Perimeter architecture within its Secure Access platform and inclusion as an add-on within its Access Suite.
- **Scytale:** announced Scytale Enterprise, a cloud-based subscription to standardize and accelerate service authentication across cloud, container, and on-premise infrastructure.
- **SSH:** introduced new container capabilities for PrivX, its access management solution, and Universal SSH Key Manager, its SSH key management and control system.
- **Unisys:** announced the availability of Unisys Stealth(identity), a biometric identity management software for biometric enrollment processing.
- **Venafi:** released research uncovering marketplaces for TLS certificates sold individually and packaged with a wide range of crimeware.
- **VeriClouds:** launched Local Service Device, a hardware device that extends its compromised credentials detection services.
- **Xton:** released XTAM Hybrid Access Security Broker software to provide secure access control for corporate network and cloud infrastructure.

Internet of Things

- **Cloud Security Alliance:** released the first IoT Controls Framework, which introduces base-level security controls required to handle IoT security risks.
- **Cyxtera:** launched IoT Connector, a feature within AppGate SDP that secures unmanaged and undermanaged IoT devices.
- **SentinelOne:** unveiled SentinelOne Ranger, an endpoint detection service for IoT that turns endpoints into detection devices and uses the same IT codebase for IoT.

Messaging Security

- **Agari:** detailed business email compromise attacks by Scarlet Widow over the past few months on thousands of nonprofits, schools, and universities.
- **FireEye:** announced an update to FireEye Email Security, integrating SEG functionality including antivirus, anti-spam, signature-based anti-malware, and impersonation protection.

Mobile Security

- **Crowdstrike:** introduced Falcon for Mobile, a threat detection and response system for mobile devices.
- **Lookout:** launched the Post-Perimeter Security Alliance in partnership with Blackberry, Google Cloud, Okta, SentinelOne, VMware, and others to provide security and productivity for the perimeter-less, cloud-delivered, and privacy-focused world.

MSSP

- **DFLabs:** announced a new version of its IncMan SOAR platform for MSSPs and MDR service providers to centrally perform one-to-many operations across multiple customer environments and provide deployment options for regulatory compliance and granular reporting analytics.
- **Malwarebytes:** launch OneView, a new multi-tenant management console for MSPs for customer protection and remediation.
- **Microsoft:** launched Microsoft Threat Experts, a managed threat hunting service within Windows Defender ATP.
- **Tripwire:** announced the expansion of Tripwire ExpertOps to include vulnerability management as a managed service.

Network and Infrastructure Security

- **A10 Networks:** announced capacity enhancement to 500 Gbps for Thunder 14045 TPS, an attack traffic mitigation system.
- **Awake Networks:** launched Ava, a privacy-aware security expert system to enhance its network traffic analysis solutions.
- **Axonius:** named winner of "Most Innovative Startup 2019" for RSAC Innovation Sandbox Contest.
- **Blue Hexagon:** announced an integration with Carbon Black for accelerated threat protection against malware attacks.
- **Citrix:** announced new capabilities in its SD-WAN solution that enable enterprises to administer user-centric policies across branches and employees.
- **Cyberinc:** released Isla Isolation Platform 4.0 with expanded capabilities in credential theft protection and availability of cloud, on-premise, and hybrid deployments.
- **Ivanti:** announced Ivanti Security Controls, a patch management solution for operating systems and third-party applications on physical and virtual servers and desktops.
- **Untangle:** introduced its Network Security Framework for enterprise security orchestration.
- **VMware:** unveiled Service-defined Firewall, an internal firewall that combines the capabilities of NSX virtualization and App Defense workload protection.

Privacy

- **BigID and Immuta:** announced partnership to deliver an integrated solution for the automation of privacy-centric data science initiatives.
- **NIST:** stated that new Privacy Framework, due in October, is being developed to be risk-based and outcome-based, rather than prescriptive.

Quantum Computing Security

- **ISARA:** announced new tools to test and implement crypto-agility and quantum-safe cryptography directly into existing systems.

Risk & Compliance

- **Bitsight:** launched Peer Analytics, a feature on its platform that allows the comparison of security performance across global organizations.

- **CyberSaint:** announced open API integrations to utilize legacy GRC technologies in CyberStrong's integrated risk management platform.
- **Cytegic:** announced support of FAIR in the assessment and quantification of cyber risk impact within its Automated Cyber Risk Officer suite of tools.
- **Optiv Security:** announced its Risk Transformation Service, an end-to-end risk assessment solution that includes strategy execution.
- **RiskRecon:** announced partnership with RSA for joint sales and marketing on third-party vendor digital risk management.
- **Spirent:** announced availability of its CyberFlood Data Breach Assessment solution for continuous automated assessment of security and DLP policies.

Security Operations

- **Chronicle:** launched Backstory, which is based on Google's internal threat detection and is built on Google's infrastructure, to store, index, and search unlimited security telemetry for corporations.
- **Exabeam:** announced Exabeam SaaS Cloud, a hosted cloud offering which provides log management and user behavioral analytics, as well as data lake and case management capabilities.
- **ISACA:** released State of Cybersecurity 2019 Survey, showing short supply of cybersecurity professionals, difficult retention even with enticements such as training and certification, declining and less effective gender diversity programs, and slight slowdown in cybersecurity budget growth.
- **JASK:** announced advanced analytics for its ASOC platform to process the high-volume data unique to AWS and Microsoft Azure cloud environments.
- **Microsoft:** rolled out Azure Sentinel, a new cloud-native SIEM tool to reduce noise and alert fatigue.
- **PagerDuty:** announced PagerDuty for Security Operations, a solution for security and developer teams including integrations from PagerDuty's partner ecosystem.
- **Palo Alto Networks:** introduced Cortex, an AI-based continuous security platform; Cortex XDR, a detection, investigation, and response product; and Traps version 6.0 with a Behavioral Threat Protection engine.
- **Polyswarm:** announced availability for its marketplace for threat detection to enterprises and MSSPs.
- **RSA:** announced new features with NetWitness Platform 11.3, including machine learning models based on endpoint observations and user behavior anomaly detection.
- **SecBI:** launched an automated cyber threat detection and response solution for MSSPs.
- **Secureworks:** launched its Orchestration and Automation solution that uses security operations expertise, security orchestration technology, managed services, and incident response experience for workflow automation and incident contextualization.
- **STEALTHbits:** announced StealthDEFEND v2.0, with new features such as support for 15 new Active Directory attack TTPs, additional response playbook actions, and contextual resource tagging.
- **Titan IC:** unveiled next generation Regular Expression Processor, which accelerates SNORT or similar IDS/IPS architectures from 10 Gbps to 100 Gbps.
- **Unisys:** announced Unisys Stealth 4.0 security software suite, which integrates with LogRhythm SIEM and fully integrates with Palo Alto Networks' Panorama network security management console.

Threat Intelligence

- **Everbridge:** announced integration IBM QRadar to provide joint customers a system for threat intelligence and automated IT response and alerting.

- **FBI:** said in RSA keynote that US had not seen a "material impact on election infrastructure" from foreign adversaries in the recent midterm elections but that foreign influence campaigns have continued "virtually unabated."
- **FBI:** cited in RSA keynote an uptick in cyber threats from Russia, Iran, China, and North Korea and an increase in "blended" attacks, where nation-states are partnering with cyber criminal gangs to attack the U.S.
- **FireEye:** published annual M-Trends report on attacker dwell times, attack trends, and offensive and defensive trends, showing a continued year-over-year decline in median global dwell time to an all-time low of 78 days.
- **FireEye:** announced the global availability of Expertise On Demand for access to Mandiant frontline experts, threat intelligence, and services.
- **Intsights:** announced a new threat evolution timeline that aggregates and correlates ongoing changes to suspicious domains into a single timeline and provides custom alerting algorithms.
- **Mimecast:** announced the Mimecast Threat Center, a group of cybersecurity experts to provide threat intelligence to organizations leveraging email, web, and anonymized user data.
- **Recorded Future:** announced Recorded Future Express, a browser extension to provide threat intelligence over existing security workflows.
- **Verodin:** announced its new Threat Actor Assurance Program in partnership with Anomali, Flashpoint, and Intel 471 to deliver threat intelligence.

Venture Capital

- **eSentire:** raised $47M led by Warburg Pincus to provide AI-powered managed detection and response.
- **Obsidian Security:** raised $20M led by Wing for machine learning-based intelligent identity protection platform.
- **Socure:** raised $30M led by Scale Venture Partners for identity verification and fraud prevention services.
- **Stellar Cyber:** Raised $13M led by Valley Capital Partners for unified security analytics.

Web Security

- **Ericom:** announced that Ericom Shield, its remote browser isolation solution against phishing, incorporates intelligence capabilities including sophisticated algorithms, URL filtering capabilities, and smart business logic.
- **SafeGuard:** launched a new detection capability for real-time, cross-channel analysis and proactive scans across deep web sites, the dark web, and the social internet.