The New Threat Landscape

- Limited cooperation between governments
- No rules of engagement in cyber warfare
- The rise of anonymous cryptocurrencies

The Rise of Professional Hacking Groups
The Rise of Ransomware
The New Adversary

- Motivated and capable
- Scalable and organized
- Highly advanced
The Growing Ransomware Threat

**BUSINESS IMPACT**
1 in 10 businesses close due to a ransomware attack

**RISING PAYMENTS**
Average payment increased upwards of 180% from March 2019 to March 2020

**RAPID DEPLOYMENT**
Median of only 3.5 days from intrusion to deployment

**AVERAGE COST**
Wide range from $250,000 to $50 million USD

**PROLIFERATING DEMAND**
Mandiant ransomware response engagements increased 10x in 2020 from 2018

Ransomware Incident Response Investigations by Mandiant

- 2018: 100
- 2019: 500
- 2020: 1000
Cyber Threats vs. Organizations’ Challenges

- The Rise of Professional Hacking Groups
- The Rise of Ransomware
- Cloud Adoption
- Skill Shortage
- Budget and Effectiveness
Side Effects of a Breach

Stunted Growth
A breach can stall a company's growth for up to 3 years

Reduced Stock Price
Average stock price decline of 3% – 7.5% after breach disclosure

Incurred Cost
Average cost of a data breach is ~$4 million USD or ~$150 USD per lost record

Lost Customers
Breaches cause abnormal customer turnover of 3.9% on average
The Four Questions for Every Security Team

Am I protected?
Have I been breached?
How do I respond?
How do I prepare?
Security and Business Outcomes

Am I protected?
- Simplified compliance and internal reporting

Have I been breached?
- Shorter time to respond and remediate

How do I respond?
- Reduced losses and reputational damage

How do I prepare?
- Improved talent retention and performance
- Higher ROI from security investments
Getting to The Truth

OUR DIFFERENTIATION

Through our expertise, intelligence and technology we learn, before anyone else, the tools and tactics attackers are using to circumvent security safeguards.
The FireEye Difference

11+ years of investigative expertise
500+ consultants in 20+ countries
400+ Red Team Exercises per year

MACHINE INTELLIGENCE
15,000 network sensors
18M Endpoints
Tens of millions of malware detonations per hour
65M Emails Processed / Day

ADVERSARY INTELLIGENCE
23 countries
30+ languages
180+ analysts and researchers
30K intel reports per year

OPERATIONAL INTELLIGENCE
5 Security Operations Centers
99M+ events ingested
21M+ alerts validated by Intel

EXPERTISE FROM THE FRONT LINES
16+ years of investigative expertise
500+ consultants in 20+ countries
400+ Red Team Exercises per year

WHO
WHY
HOW
IMPACT

850 ENGAGEMENTS
200K HOURS
RESPONDING TO ATTACKS PER YEAR

Breach Intelligence
- Global campaign
- By a highly capable threat actor
- Involves numerous vendors
- Targeting many state agencies
- FireEye caught it first

FireEye UNC2452 and Sunburst online Resource Center
Solutions that enable every security team in the world to easily **augment** and **automate** our intelligence and expertise into their environment, regardless of the controls they have deployed.

Solutions with **detection**, **protection**, and **response** capabilities under a security operations platform, Helix, powered by intelligence and expertise from Mandiant.
Mandiant Solutions Portfolio
The goal of Mandiant Solutions is to **augment and automate** every security team in the world with expertise and intelligence, regardless of SIEM/controls deployed.

- Consulting Services
- Threat Intelligence
- Security Validation
- Defense (formerly Respond)
- Managed Defense
- Expertise On Demand
- The portal to all things Mandiant
- SaaS offering
- Integration across solutions
Business Outcomes

- Focus on the highest-risk issues: Prioritization
- Better leverage existing security controls: Optimization / Rationalization
- Identify important context automatically: Efficiency
- Validate your adversary-specific controls: Understand Relevance & Readiness
- Proactively hunt for key adversaries: Decrease Damage / Peace of Mind
- Intelligence overlaid on Sec Ops workflow: reduce impact
- Better leverage existing security controls: Optimization / Rationalization
Focus on threats that matter to your business right now

- Optimize resources. Realign cyber defense strategy based on latest insights.
- Early warning on brand or reputation threats.
- Reduce attack surfaces based on exploit and prevalence ratings.
Why Mandiant Threat Intelligence

**Direct access** to Breach, Machine, Operational and Adversarial Intelligence

**Threat Visibility**
Global, geo, industry… your brand

**Relevant & actionable**
Trends, actor profiles, tactics, observables, reports …

**Attribution & Adversarial Graduation** (Temp, APT, FIN)

**Time to value**
SaaS offering with enablement and expertise

**Easy to integrate** with any security tool
Mandiant Security Validation

Know the true measure of your security

- Understand how your defenses perform against real adversary attacks
- Gain evidence of effectiveness of security controls
- Measure performance against Industry Frameworks
The Five-Step Framework of Mandiant Security Validation

Continuous monitoring, validation, and optimization of your security program

Prioritize
- Proactively identify threats
- Use real-world adversary tactics, techniques, and procedures rather than simulations
- Use comprehensive threat coverage with an equal focus on both technical attacks and adversary tactics across multiple attack vectors

Measure
- Gather quantitative evidence of effectiveness
- Use precise knowledge to drive improvement
- Assess security infrastructure health

Optimize
- Gain specific controls-based visibility
- Improve effectiveness of security tools
- Shift to proactive testing with real, full lifecycle attacks

Rationalize
- Leverage definitive proof of control performance
- Measure impact values to security posture
- Apply quantitative data to ROI analysis

Monitor
- Maintain confidence with operationalized effectiveness
- Avoid deviations in performance
- Inform with automated monitoring & reporting
Mandiant Consulting Overview

Incident responder of headline breaches since 2004

Powered by frontline threat intelligence and purpose-built technology

500+ consultants in 20+ countries

Remote and on-premise rapid incident response

Assessment, Transformation, Defense, and Training services
Mandiant Consulting Services Portfolio

Assess to answer
- Is there attacker presence?
- Am I prepared to respond?
- How effective is my security posture?

Defend
- Expert-driven detection and response
- 24 x 7 protection
- Industry-leading detection and intel

Transform to mature security
- Security program review and improvement
- Processes optimization
- Implementation support

Train to develop your capabilities
- FireEye solutions education
- Cyber security education
- Threat space cyber range
Mandiant Defense

SOC Investigation at Machine Speed

- Reduce response time and security engineering costs
- Accelerate analyst productivity
- Detect more incidents
- Handle incidents in IT/OT

>1 Trillion events processed

1.1 billion worthy of investigation

<10,000 incidents escalated
The XDR Engine

What It Does

- Gathers evidence from siloed sensors
- Automatically incorporates company specific context
- Triages 100% of alerts
- Groups all events and alerts into one incident
- Takes feedback and adjusts automatically

Benefits

- Leaves data where it is
- Accurate and consistent
- Massive reduction in false positives
- Fast investigation-to-escalation
- Rules not required reducing engineering time and costs
- Controls agnostic - leverage best-of-breed solutions
Managed Detection and Response (MDR) service delivered by frontline defenders that augments your team and elevates your security posture.

**Expose Adversaries**
Enlist elite threat hunters using nation-grade cyber threat intelligence to proactively hunt across security controls and surface relevant threats.

**Accelerate Response**
Respond to attacks before they disrupt your business with the collective knowledge and experience of Mandiant.

**Elevate Your Defenses**
Gain a team of cybersecurity experts who can augment your security program with tailored recommendations.
How Managed Defense Works

1. Technology Alerts
2. Enrich with Mandiant Threat Intelligence
3. Surface threats and prioritize relevant alerts
4. Analytics & Advanced Threat Hunting
5. Contain compromised assets, scope incidents and remediate
6. Publish investigations with findings and recommendations

Security Technology | Detection | Response
--- | --- | ---
Technology Alerts | Enrich with Mandiant Threat Intelligence | Surface threats and prioritize relevant alerts
Analytics & Advanced Threat Hunting | Contain compromised assets, scope incidents and remediate | Publish investigations with findings and recommendations
Mandiant Expertise On Demand

Flexible access to a wide range of industry-recognized Mandiant security expertise.

- **Amplify your team** with side-by-side access to proven skills and threat insight.

- **Increase situational awareness** via Daily News Analysis, Quarterly Threat Briefings and our Ask An Analyst feature.

- **Advance your security program** and capabilities via training and consulting services.

- **Gain a single, trusted partner** with unrivaled breadth and depth of cyber security experience and skills.
Mandiant Expertise On Demand

Expertise On Demand is an annual subscription that provides flexible access to the expertise organizations need, when they need it.

- **Ask An Analyst**
  Ask Mandiant analysts for help answering your toughest security questions at any time.

- **Fixed-Scope Mandiant Services**
  Request, develop and extend expertise with flexible access to investigations, intelligence, training and consulting services.

- **Included in All Subscriptions**
- Daily News Analysis Emails
- Quarterly Threat Briefs
- Mandiant IR Retainer (Optional SLA Available)
FireEye Products Portfolio
The goal of FireEye is to **catch** advanced threats across all major threat vectors before they can cause damage and **empower** teams with the critical tools for their security operations.
FireEye Helix

Technology
- Next-Gen SIEM
- Behavior Analytics
- Cloud Visibility

Processes
- Automation
- Guided Investigation
- Compliance Reporting

Expertise
- Expertise On Demand
- Threat Intelligence
- Risk Prioritization
FireEye Helix Overview

- Real-time threat intelligence
- Codified expertise from FireEye
- Sub-Second search
- Single log source
- Guided investigations
- Compliance reporting
PROTECTION FOR #1 THREAT VECTOR

- Stops advanced threats, impersonation, and phishing attacks

- Protects in the Cloud, on premises, and across major solutions like O365 and G-Suite

- Applies Mandiant Threat intelligence for advanced detection and context
FireEye Email Security

Superior efficacy in detecting and stopping advanced email-borne threats.
FireEye Endpoint Security

- Stop malware and advanced attacks
- Detect breaches that bypass security
- Respond to the threats quickly, completely, and at scale
Endpoint Security – Technology

- Malware Protection (MP)
- ExploitGuard (EG)
- MalwareGuard (MG)
- Real Time IoC (RT)

1. Initial Reconnaissance
   - Initial Compromise
   - Establish Foothold

2. Maintain Presence
   - Move Laterally
   - Escalate Privileges
   - Internal Reconnaissance

3. Complete Mission

- Automatic Block & Quarantine
- Advanced Detection
- Containment
Endpoint Security MITRE ATT&CK

- MITRE ATT&CK framework replicates real-world
  - Becoming de-facto standard in the industry
FireEye Network Security & Forensics

Provides network visibility and protection against the world’s most sophisticated and damaging attacks.

- Advanced Threat Detection
- Multiple Machine learning and correlation engines
- Full Packet Capture Capabilities
- Protection for Mac, Windows and Linux systems
- On-Premise, Virtual, Cloud and SaaS Protection
FireEye Network Security

More than a sandbox, more than an appliance...

**For Infrastructure**
The best detection regardless of form factor
North/South and East/West Coverage

**For Internal Applications**
The ability to submit files for verdict via API

**For SaaS**
The ability to leverage a web gateway solution embedded with FireEye Detection
FireEye Detection On Demand

- Objects in your cloud
- SOC
- SIEM
- Files in web applications
Journey of a Submission
FireEye Cloudvisory is a control center for cloud security management that delivers **Visibility, Compliance** and **Governance** to any cloud environment.

Available on **aws marketplace**
Cloudvisory: Differentiators At-A-Glance

1. The most advanced Visibility capabilities in the CSPM market today
2. Exception handling and in-line remediation for compliance failures
3. Cloud-native microsegmentation
4. Complete control over role permissions
Industry Recognition
Recent Awards and Certification
Common Integrations
Thank you.
FireEye’s Values

Do it Right:
We do things the right way, without cutting corners.

Be Curious:
We stay relevant by constantly learning and inventing.

Focus on Solutions:
We relish challenges and adversity. Rather than fixating on problems, we are tireless in our pursuit of solutions.

Put the Customer First:
We do what it takes to exceed our customers’ expectations. We under promise and over deliver.

Be Respectful:
We respect each other’s differences, value diversity, and listen to one another.

Execute:
We do what we say we will do.

We seek out employees with qualities that facilitate high-quality results – those traits that give personal meaning to their work. We define ourselves by our values.