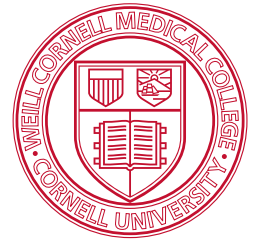


Weill Cornell Medical College

HP Enterprise Security Customer Case Study

“We’ve driven down our asset vulnerabilities by about 50% in the last two years, and we could not have done it without ArcSight ESM.”

—Benjamin Nathan, Associate Director of Security and Identity Management, Weill Cornell Medical College



Customer Brief

Founded in 1898, Weill Medical College of Cornell University is among the top-ranked clinical and medical research centers in the country. It maintains major affiliations with New York-Presbyterian Hospital, Memorial Sloan-Kettering Cancer Center and the Hospital for Special Surgery. Weill Cornell has 1,300 faculty members, 3,000 staff members and 1,000 students on campus, and sees about 1 million patients each year.

Product(s)

- ArcSight ESM

Business Benefits

- Weill Cornell uses ArcSight ESM to defend against 12,000 security attacks each year, and also expects to save \$120,000 and 3,120 hours per year in remediating compromised systems
- Insider threats such as employees accessing high-profile patient medical files, can be detected and effectively minimized
- ArcSight ESM makes it possible to monitor and report on any event and quickly demonstrate compliance to auditors



The Weill Cornell Medical College Challenge

The healthcare sector is experiencing a significant increase in the number of data breaches. Cybercriminals aren't just targeting medical records, but any kind of data that can be a source of profit, including demographic and financial information belonging to patients. Healthcare organizations like Weill Cornell must guard themselves against data breaches and other grave threats, and also comply with a slew of regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and new rules placed on HIPAA as part of the Recovery Act.

To preserve the integrity of patient data and reduce overall risk, Weill Cornell needed to understand what was happening on its network at all times. Moreover, it needed to connect the dots across all network activity to detect sources of risk and eliminate potential problems.

Weill Cornell also faced some unique security challenges. Namely, it had to juggle the often-conflicting demands of regulatory compliance and academic freedom. In academia, data needs to be easily shared and transmitted; data access can't be restricted because of concerns over security and regulatory compliance.

HP Enterprise Security Customer Case Study:

Weill Cornell Medical College uses ArcSight ESM to intelligently correlate event data, meet compliance requirements and mitigate network threats.

Industry: Healthcare



"There is a greater need for our doctors and patients to be able to communicate anytime and anywhere, to share medical data in new ways, and to have medical data transferred effectively," explains Benjamin Nathan, Associate Director of Security and Identity Management at Weill Cornell Medical College. "If our doctors want to use new technologies that make it easier to share information, such as Facebook or Google Docs, we have to figure out how to facilitate that without compromising the integrity of our data."

The ArcSight Solution

Weill Cornell generates millions of log events each day from dozens of sources, including servers, databases, vulnerability scanners and anti-virus systems. The healthcare organization embarked on a rigorous selection process, ultimately choosing ArcSight ESM to intelligently correlate event data, meet compliance requirements and mitigate network threats.

"ArcSight ESM is an out-of-the-box solution that's perfectly suited to our needs," says Nathan. "We have a small team, so the automation within ArcSight ESM is critical. The system only reacts to events and anomalies that really matter, which means we don't have to waste our time and resources chasing down false alarms."

Weill Cornell is leveraging ArcSight ESM for a number of use cases that go far beyond standard perimeter security. ArcSight ESM maps directly to HIPAA and other regulations, which means Weill Cornell can monitor and report on any event and quickly demonstrate compliance to auditors. Weill Cornell will also be gaining new insight into insider activity, including all potential threats against its electronic health records systems. Finally, the organization has broadened the scope of its security efforts to include the physical layer. Specifically, it is using ArcSight ESM to monitor event logs from badge readers and swipe cards, ensuring that only the right people are gaining access.

The ArcSight Impact

ArcSight ESM has allowed Weill Cornell to recognize meaningful metrics around its security and compliance posture.

Defending against Cyberthreats

"With ArcSight ESM, we successfully defend 12,000 security attacks per year," says Nathan. "We spend about 80 hours per week remediating compromised systems. We expect to cut that time in half within the next 12 months, then half again to 20 hours in the 6 months following. So, we'll be saving 3,120 staff hours per year, or \$120,000, just in this one area; and that's very significant to us."

"One of the real benefits of ArcSight ESM is improved visibility," Nathan points out. "We now can see the security-related incidents that otherwise would have gone unnoticed."

Tracking Asset Vulnerabilities

Weill Cornell is also able to conduct asset vulnerability tracking for critical systems that either contain confidential data or are infrastructure for other systems that do. "A breach on any of these systems – especially those containing confidential data – is an extremely bad thing for us, especially in terms of integrity and monetary ramifications for things like notifications if we were to lose patient health information and social security numbers," says Nathan.

After Weill Cornell classifies the servers by criticality, they review vulnerabilities found on those systems and assess the potential weakness. This gives them a way to prioritize which vulnerabilities are patched or otherwise remediated. "We've driven down our asset vulnerabilities by about 50% in the last two years, and we could not have done it without ArcSight ESM," says Nathan.

Protecting Patient Information

Weill Cornell is using ArcSight ESM in many other interesting and effective ways. For instance, if a curious employee accesses medical records of a high-profile patient and then prints them, ArcSight ESM can detect the incident through event correlation. ArcSight ESM can then automatically identify and place the user on a watch list it creates on the fly. Such tracking and escalation makes it possible to detect additional policy violations or suspicious activity by that user, such as copying sensitive data to a USB drive.

"Each of those events individually is not nearly as important as all those events occurring simultaneously," explains Nathan. "ArcSight ESM can tell us when something much more significant than normal is happening."

Stopping Identity Theft

ArcSight ESM correlation capabilities also help to prevent identity theft. If a billing application manager is viewing an unusually large amount of medical records, it knows to pay extra attention to that user via a watch list it. If a USB drive was then inserted into that user's workstation, or a large amount of printing was done, and actions add up to a clear policy violation, functionality within ArcSight ESM can notify the appropriate personnel, open a trouble ticket and initiate forensic activity to determine the scope of the threat.

Multiple Challenges, One Solution

"Medical records privacy is one of our most visible challenges, but we also have to worry about protecting our R&D, securing the physical layer and meeting compliance regulations," says Nathan. "The ArcSight SIEM platform makes it easy to solve our entire range of monitoring and security challenges."

